

# MECHANISMS FOR NEXT GENERATION NETWORKS SERVICES INTEGRATION ACROSS HETEROGENEOUS NETWORKS



FERNANDO MENDIOROZ COTELO

Master of Science in Telematics Engineering

Director:

Álvaro Rendón Gallón

PhD in Telecommunications Engineering

University of Cauca

Faculty of Electronics and Telecommunications Engineering

Department of Telematics Engineering

Research Line in Advanced Telecommunications Services

Popayan, November of 2016

FERNANDO MENDIOROZ COTELO

MECANISMOS DE INTEGRACIÓN PARA  
PRESTACIÓN DE SERVICIOS DE NUEVA GENERACIÓN  
SOBRE REDES HETEROGÉNEAS

Trabajo de Grado presentado a la Facultad de Ingeniería  
Electrónica y Telecomunicaciones de la  
Universidad del Cauca para la obtención del  
Título de

Magíster en  
Ingeniería Telemática

Director:  
Dr. Ing. Álvaro Rendón Gallón

Popayán, 2016

## **Página de Aceptación**





## Acknowledgement Page

I would like to express my eternal gratitude to my MSc. tutor, PhD Álvaro Rendón Gallón, for believing in this project in the first place even though it appeared ludicrously ambitious and unfeasible by the time he accepted mentoring me. Nobody but him accepted the challenge. For his continuous support on my study and related research, for his patience, motivation, and immense knowledge. His guidance helped me throughout the time of research and writing of this thesis. Some fellow students told me at the beginning I could not have a better advisor and mentor for this work. I could not agree more. Also, for his confidence for letting me take over lecturing on «Switching Systems» at University of Cauca, a superb honour.

As aforementioned, the subject of this academic adventure appeared from the start as a chimera, as either its scope was as vast as it could be, while it involved lot of issues that were out of our control. Being this an academic work, it is highly guided for the Telco industry, thus just defining the aims was a huge challenge, as we needed to go back and forth to discover something unsettled in this non-stopping business. Moreover, and despite my long-time relationships with Mobile Network Operator's staff, should they be available for testing an academic endeavour? How would we asses it? Would some of the few labs around the world dedicated to this area of knowledge accept this trial? Would there be an enterprise out there willing to make a try? After some time looking to find the answer for these questions and even returning to the industry as Innovation Manager for a Mobile Network Operator, the most amazing thing happened: co-founders of TeleStax Inc., the company behind the Open Source project we had been studying and focusing our thesis, i.e. Mobicents (now RestComm), Ivelin Ivanov (CEO), Jean Deruelle (CTO) and Amit Bhayani (COO) asked me to join their team and made me lead of the RestComm Geolocation project. What was beginning to look like a nightmare, suddenly became a dream come true. My gratefulness for the confidence put on me by these outstanding pioneers of the industry is immeasurable. Furthermore, I suddenly found myself engaged in a team of incredible talented and graceful professionals in the area of

knowledge related to this work and beyond. Hence, as extremely challenging the project remained, the ride was rewarding. Besides Ivelin, Jean and Amit, I could mention every single individual in TeleStax team to thank for. Just some special mentions to Guilherme Humberto Jansen, Jaime Casero, Sergey Vetyutnev, George Vagenas and Alexandre Mendonça for their initial push, advices and mentoring in RestComm framework, involvement in Geolocation project brainstorming and peer reviewing my work.

Becoming part of TeleStax' world also introduced me to wonderful people, all world-class professionals. We engaged in TADHack events and therefore made TADHack Uruguay possible during May of 2016 (and now planning the same for Colombia and other Latin American countries for next years). Also, after TADSummit 2015, during TeleStax' «Restconn» event in late November 2015, just some weeks after joining TeleStax, I had the pleasure to meet some amazing people that warmly embraced and encouraged me in the pursue of this life time achievement. Mark White (CEO of Locatrix), James Body and Andy Smith from Truphone. While Mark introduced me to Andrew Eross (CTO of Locatrix), both James and Andy joined him on priceless brainstorming discussions around the matter of this work. Later, long-time acquaintances like Marcelo Aranibar from Tigo Bolivia and Osmar Coronel (current CEO of American Prepaid VAS and former Millicom regional CTO for more than two decades) joined the party. Osmar then derived me to his lead software engineer, Julio Rey. Along with Jean Deruelle from TeleStax, Andrew Eross, Marcelo Aranibar, James Body and Julio Rey kindly accepted to assess this work as for DESMET methodology, even though it was a disruption of their busy schedules. Not only they did, but provided amazing feedback throughout the qualitative surveys they went through. My eternal thankfulness to all these exceptional experts.

Last but not least, I would like to thank my family members and long-time friends for their support and patience throughout this process, especially to my late dad, my mother and elder aunt for backup me emotionally throughout this work and my whole life. I wouldn't have got anywhere without your forever love and support.

## Resumen Estructurado

### Antecedentes

Tras más de una década de trabajo en investigación y desarrollo, despliegue y soporte de Servicios de Valor Agregado para operadores de redes móviles, estrictamente acotados a soluciones basadas en la pila de protocolos del Sistema de Señalización N°7, el advenimiento de estándares, paradigmas y despliegues de redes de próxima generación tales como LTE o el Subsistema IP Multimedia exige una inmediata adaptación a estas nuevas tendencias de forma de no perecer en la obsolescencia.

Teniendo presente que los Servicios de Valor Agregado funcionando en redes legadas de circuitos conmutados aún persistirán por al menos una década (especialmente en países en vías de desarrollo), el requisito ineludible de la adaptación a nuevos paradigmas como la Arquitectura Orientada a Servicios (SOA) o el Internet de las Cosas (IoT), estrechamente ligados con la aparición de nuevas tecnologías y protocolos de comunicación sobre redes de paquetes conmutados enteramente basadas en el protocolo IP, tales como SIP o Diameter, contextualizó las bases y direccionó este trabajo de investigación y desarrollo.

## Objetivos

Cuan vastos son los tópicos descriptos en los antecedentes de este trabajo, se torna imperativo limitar el alcance del mismo de acuerdo a los objetivos de un grado de maestría en investigación. Por tanto, el objetivo general de este trabajo de grado de maestría consiste en habilitar el despliegue de servicios de valor agregado en un contexto de redes de telecomunicaciones móviles heterogéneas, mediante el desarrollo de mecanismos transparentes de localización y mensajería según los organismos de estandarización internacional, con especial foco en las especificaciones 3GPP/LTE.

De forma de cumplir con el objetivo general descrito previamente, se plantearon los siguientes objetivos específicos:

1. Seleccionar un entorno de trabajo de código abierto, que incluya una plataforma de despliegue de servicios y ambientes de prueba/simulación de redes, con capacidades para la construcción de soluciones para redes de telecomunicaciones heterogéneas.
2. Desarrollar una interfaz de programación de aplicaciones (API) y complementar los adaptadores/habilitadores de recursos de red, de modo de proveer alternativas a actuales omisiones tanto de la plataforma seleccionada como de las especificaciones en desarrollo para servicios de mensajería y localización, para proveer un funcionamiento transparente en redes heterogéneas, ya sea para acceso en redes legadas como de próxima generación.
3. Desarrollar un prototipo y configurar el ambiente de prueba/simulación para validar los servicios utilizando métodos de evaluación según la metodología DESMET [100].

## Métodos

Dado que este proyecto se ha concebido en general bajo «Enfoque del Marco Lógico» [92], ciertos productos son descriptos para cada uno de los objetivos específicos.

En lo concerniente al primer objetivo específico, i.e. «seleccionar un entorno de trabajo de código abierto, que incluya una plataforma de despliegue de servicios y ambientes de prueba/simulación de redes, con capacidades para la construcción de soluciones para redes de telecomunicaciones heterogéneas», las siguientes son las actividades programadas para su cumplimiento:

- Investigar de acuerdo a publicaciones en revistas indexadas y/o conferencias relacionadas al objetivo planteado, los entornos de trabajo (plataformas de despliegue de servicios y ambientes de prueba/simulación de redes) que conllevaron a casos de relativo éxito alineados con el objetivo general.
- Investigar ventajas y desventajas, aportes y brechas de los entornos de trabajo existentes en relación al objetivo planteado.
- Investigar la viabilidad de despliegue en un ambiente industrial en términos de confiabilidad, robustez, escalabilidad, flexibilidad, etc.
- En consonancia con los objetivos y arquitectura del proyecto de laboratorio NGN/IMS o «Telco 2.0» del grupo GIT de la Universidad del Cauca, estudiar la viabilidad de integrar a dicho proyecto la plataforma de desarrollo y despliegue de servicios seleccionada.

En lo concerniente al segundo objetivo específico, esto es, «complementar los adaptadores/habilitadores de recursos de red de modo de proveer alternativas a actuales omisiones tanto de la plataforma seleccionada, como de las especificaciones en desarrollo para USSI y LCS sobre IMS y LTE», las siguientes son las actividades programadas para su cumplimiento:

- Desplegar la plataforma de despliegue de servicios de código abierto seleccionada y comprobar los correctos funcionamientos de sus capacidades, habilitadores y adaptadores de recursos para MAP, SIP y Diameter.

- Establecer los canales de comunicación pertinentes para la prestación de soporte y colaboración con los desarrolladores de la plataforma seleccionada.
- Desarrollar las aplicaciones informáticas necesarias para soportar una API que habilite servicios basados en localización independientemente del canal que los dispare. Más específicamente, implementación de los complementos a la API y adaptadores de recursos de la plataforma de despliegue de servicios seleccionada, de acuerdo a las normas de 3GPP/LTE para mensajería y localización, que permitan la transparencia para el usuario del servicio en redes de acceso móvil heterogéneas.

En lo concerniente al tercer objetivo específico, esto es, «desarrollar un prototipo y configurar el ambiente de prueba/simulación para validar los servicios utilizando métodos de evaluación según la metodología DESMET», las siguientes son las actividades programadas para su cumplimiento:

- Producir un entorno controlado de pruebas de los servicios mediante el despliegue de la arquitectura de red necesaria para el funcionamiento/simulación de servicios de valor agregado de telefonía móvil. Para esto se contaba al inicio del proyecto con la iniciativa en curso del GIT de la Universidad del Cauca del proyecto de laboratorio NGN/IMS «Telco 2.0» y plataformas de prueba/simulación de redes de software libre como las referenciadas en [53, 83-90] (y de este modo, establecer un ambiente de simulación de entidades e interfaces de red conformes al objetivo general del proyecto). Finalmente, se utilizaron las herramientas, entorno de pruebas y procedimientos de aseguramiento de calidad de TeleStax detallados en [122].
- Diseñar y desarrollar servicios convergentes de acuerdo a los escenarios de motivación descritos, a saber:
  - Disparar Servicios de localización mediante las extensiones del protocolo Diameter de acuerdo a [43-45] para LTE o mediante operaciones MAP [22] vía múltiples medios como USSDI/USSI originado en el móvil (MO) u originado en la red (NI) o servicios Web REST.
- Selección de una o más de las metodologías DESMET para la evaluación de extensiones y Servicios desarrollados de acuerdo a los siguientes criterios:

- Conformidad de la API y los adaptadores de recursos para USSD y LCS, respectivamente sobre SIP y Diameter, implementados en la plataforma de despliegue de servicios seleccionada, con los lineamientos de 3GPP TS 24.390 [42] y 29.172/3 [44-45].
- Aplicabilidad y/o factibilidad para la expansión y/o migración de servicios de valor agregado innovadores en ambientes de producción a nivel industrial.
- Viabilidad y calidad de impacto para los objetivos planteados por los escenarios de motivación del proyecto, i.e., la Red Nacional de Telecomunicaciones de Emergencia para LTE (RNTE) del Ministerio de las TIC de la República de Colombia, los lineamientos de Servicios Financieros Móviles (SFM) de la Comisión de Regulación de Comunicaciones de la República de Colombia, los servicios 911 de próxima generación (NG911) de la Asociación Nacional de Números de Emergencia (NENA) de los Estados Unidos de América, o la «Ley Stalker» del gobierno del Perú.
- Establecer contacto con grupos de investigación y desarrollo de empresas o instituciones académicas involucrados en proyectos análogos, que puedan contribuir en el proceso de desarrollo y validación de la plataforma.

## Resultados

Como resultado de las actividades llevadas a cabo, se han aportado los siguientes productos, disponibles para toda la comunidad de desarrollo de software para telecomunicaciones, dada la naturaleza de código abierto de los desarrollos:

- Primera API de geolocalización de código abierto para interacción con redes móviles y acceso a datos de localización bajo redes de acceso de radio celular y/o WiFi: «RestComm Geolocation API». El diseño y la plataforma elegida para el desarrollo de la API, permiten además agregar valor a nuevos o pre-existentes servicios en redes heterogéneas. En otras palabras, la información de localización móvil puede obtenerse autónomamente o dispararse por

eventos asíncronos desde servicios de mensajería, voz, etc., independientemente de la infraestructura de red subyacente. De acuerdo a la evaluación final, se destacan las siguientes cualidades para la «RestComm Geolocation API»:

- Definición, diseño y documentación de la API íntegramente comprensible para desarrolladores Web sin previos conocimientos en la materia.
  - Definición, diseño y documentación del lenguaje de descripción RCML («RestComm Markup Language») íntegramente comprensible y adecuado a un entorno de creación de servicios de telecomunicaciones o SCE («Service Creation Environment») tal como el RVD («RestComm Visual Designer»).
  - Provisión de un entorno amigable de creación de servicios basados en localización, con formatos apropiados para la solicitud (i.e. cURL) y captación de información (i.e. XML o JSON).
  - Provisión de una solución bajo el paradigma de «Arquitectura Orientada a Servicios» a desarrolladores sin conocimientos previos sobre protocolos infraestructura de redes subyacentes de telecomunicaciones.
  - Captura de información de localización de dispositivos móviles en dos modos: inmediato y disparado por eventos.
  - Interacción adecuada con pasarelas de localización móvil en redes celulares o GMLC, ya sea propio (RestComm GMLC) como de terceras partes -bajo los lineamientos 3GPP/LTE y OMA MLP-, así como kits de desarrollo de software para aplicaciones itinerantes en redes WiFi.
- Liberación de primera plataforma GMLC de código abierto de acuerdo a los lineamientos de grupos de estandarización internacional como 3GPP y OMA, para obtención de datos de información de localización móvil bajo cualquier red de acceso. De acuerdo a la evaluación final, se destacan las siguientes cualidades del «RestComm GMLC»:
    - Cumple con las últimas tendencias para la obtención de información de localización de dispositivos móviles tanto en redes legadas como de próxima generación.
    - Cumple con las necesidades de un nodo cliente mediante el uso de solicitudes HTTP (GET/POST) y OMA MLP [107].
    - Provee servicios bajo estándares de performance «Carrier Grade».



- Cumple con los lineamientos de las especificaciones 3GPP/LTE para la obtención de información de localización en redes celulares legadas de segunda y tercera generación como GSM y UMTS en tanto éstas dispongan de mecanismos de posicionamiento adecuado (i.e. la ubicación de un nodo SMLC y métodos de posicionamiento como OTDOA).
- Cumple con los lineamientos de las especificaciones 3GPP/LTE para la obtención de información de localización en redes celulares de cuarta generación celular como LTE/LTE-Advanced en tanto éstas dispongan de mecanismos de posicionamiento adecuado (i.e. la ubicación de un nodo E-SMLC y métodos de posicionamiento como OTDOA).
- Único desarrollo de código abierto de las interfaces Diameter SL<sub>h</sub> y SL<sub>g</sub> para localización de equipamiento móvil bajo cobertura LTE de acuerdo a los lineamientos de las normas de 3GPP/LTE.
- La combinación de la RestComm Geolocation API y RestComm GMLC (provisto de las interfaces Diameter descritas en el punto anterior), comprende una solución completa pero aun expandible para la provisión de servicios basados en localización disparados por cualquier tipo de evento asíncrono, ya sea vía servicios Web REST o métodos de mensajería clásicos de telefonía móvil como SMS y USSD, satisfaciendo las necesidades de los escenarios de motivación descritos en [36-38, 105-106], independientemente del equipamiento utilizado o la red de acceso.

## Conclusiones

Tras una muy ambiciosa iniciativa de trabajo y luego de acotar el alcance del proyecto de maestría a objetivos realizables, los objetivos generales y específicos planteados han sido alcanzados dentro de un marco de trabajo ideal, dada la adopción de TeleStax, la empresa detrás del proyecto de código abierto de comunicaciones más extendido globalmente, i.e. RestComm (sucesor de Mobicents).

Es importante apuntar que la realización del proyecto conllevó un trabajo muy arduo, dado el contexto histórico durante el cual el mismo fue llevado adelante. A diferencia de décadas anteriores, los operadores de telecomunicaciones móviles ya no se encuentran en las condiciones ventajosas de la época previa a la incursión de los OTT («Over-The-Top»). Es así, que toda iniciativa de innovación que implique costos es mucho más difícil de llevar adelante que en épocas pretéritas, durante las cuales las ganancias de los operadores era tal, que aquellos bríos de investigación y desarrollo que implicaran incertidumbres, igual normalmente contaban con oportunidades de realización. La irrupción de la telefonía IP y los mencionados OTT han cambiado las reglas de juego dramáticamente. En función de que los objetivos de este trabajo claramente apuntan al despliegue de soluciones sobre redes de telecomunicaciones móviles y específicamente, operadores de telefonía móvil, convirtió la tarea prácticamente en una quimera. Irónicamente, este contexto lejos de bloquear el proyecto, a largo plazo terminó beneficiándolo. A continuación, explicaremos los motivos.

Las grandes compañías de telecomunicaciones, ya sean operadores como vendedores, han tenido que ajustarse a los tiempos de enormes cambios de paradigmas tecnológicos. En un contexto financiero desfavorable, estos grandes jugadores de acciones públicas, empiezan a mirar con buenos ojos iniciativas de código abierto, ya comprobadamente exitosas (e.g. Linux, JBoss, Hadoop, Cloudera, etc.). TeleStax y su portafolio de productos RestComm caen dentro de esta categoría, por lo que contribuir al proyecto en este marco da como resultado una vía de acceso al mundo de las operadoras móviles, prácticamente inaccesible desde una iniciativa académica. Dicho lo anterior, también constituyó un enorme desafío incorporar una funcionalidad no planificada en el medio de un camino trazado para una empresa como TeleStax cuyo objetivo primigenio es establecerse como el principal agente de telefonía IP en la nube. Una laboriosa presentación muy bien valorada en el evento Restconn 2015 [E10-E16] terminó de despejar el camino en este sentido.

Durante el diseño y desarrollo del trabajo, surgieron muy bienvenidos aportes tanto de la comunidad sostenida por TeleStax (nacida a partir del surgimiento del proyecto Mobicents), así como de socios y clientes de la organización. Fue así que el trabajo contó con aportes valiosos desde estas fuentes y también por este motivo

pudo obtenerse una evaluación de parte de destacados profesionales afines al área de conocimiento del presente proyecto. De esta forma, una idea nacida en un ámbito meramente académico, más allá de la experiencia laboral en el área de quien elabora este trabajo, concluye en un proyecto de índole industrial. Más aún, el proyecto no termina con esta tesis académica, sino que abre las puertas a la continuación del mismo para el agregado de funcionalidades y ramificaciones. Finalmente, dado que el proyecto se encuadra dentro de un marco de código abierto soportado por una vibrante comunidad, el espacio para proyectos académicos relativos al área de conocimiento en cuestión queda abierto de par en par. De esta forma, queda establecido el espacio para la continuidad de este proyecto no sólo desde la perspectiva industrial, pero incluyendo el ámbito académico.

Desde la perspectiva industrial, los productos de este trabajo están siendo considerados por operadores de telecomunicaciones para su integración en sus redes, lo cual obviamente satisface las expectativas creadas al iniciar el trabajo. Parte de estas iniciativas están siendo directamente tratadas con los operadores, en tanto otras a través de empresas asociadas (en parte evidenciado en las encuestas cualitativas utilizadas para su evaluación de acuerdo a la metodología DESMET). También, los productos de este proyecto se encuentran enmarcados en un proyecto de servicios financieros móviles en países en desarrollo en África y Latinoamérica, donde la obtención de información de localización en tiempo real resuelve numerosos asuntos de interés de departamentos de aseguramiento de ingreso y fraude, así como mercadeo en lo relativo al despliegue de promociones por zonas geográficas. Del mismo modo, los reportes de localización disparados por eventos introducidos en este trabajo, permiten el seguimiento de los clientes de forma de alertar y/o prevenir el uso indebido de mensajería promocional.

Adicionalmente, dado el rol del autor de este trabajo en la empresa TeleStax y sus vínculos académicos, tal como fue advertido en el párrafo anterior, existe la intención de promover y asistir proyectos de investigación y desarrollo en el ámbito académico en las áreas de conocimiento afines. Esto involucra por supuesto a la Universidad del Cauca o cualquier institución del país que desee participar. Proyectos nacionales como los mencionados bajo los escenarios de motivación (RNTE y SFM) se ajustan perfectamente a este tipo de iniciativas de colaboración académica-empresarial. Otros proyectos en los que la Universidad del Cauca ha

mantenido una participación decisiva como «Tucan3G» [E17-E18], podrían perfectamente ajustarse, por ejemplo, para proveer información de localización en tiempo real para asistencia médica de emergencia en zonas rurales apartadas. En el mismo sentido, se vienen manteniendo conversaciones con el equipo de investigación del «Illinois Institute of Technology» para aquellos proyectos afines a servicios de emergencia de próxima generación (NG911) de la Asociación Nacional de Números de Emergencia (NENA) de los Estados Unidos de América [105] en dicha universidad, específicamente con los participantes del trabajo relativo a la obtención de información de localización civil desde teléfonos móviles en ambientes cerrados [139].

Concluyendo, como resultado de este trabajo, realizado en el marco de la plataforma de software para telecomunicaciones de código abierto más importante y activa a nivel global (tal como puede verificarse en [E19-E20]), además de alcanzar los objetivos planteados, se ha plantado la semilla para la continuidad y expansión del proyecto tanto a nivel industrial como académico. Referirse al capítulo 7 de este documento para más detalles sobre los trabajos planteados a futuro.

**Palabras Clave:** HetNets, Servicios Basados en Localización, MAP, Diameter, SIP.

## Structured Abstract

### Background

After working on research and development, deployment and support of Value-Added Services for Mobile Network Operators for more than a decade, strictly reduced to solutions based on Signaling System N°7 protocol stack, the advent of Next Generation Network standards, paradigms and deployments such as Long Term Evolution and the IP Multimedia Subsystem, adjusting to these new trends became an immediate need, so as not to perish in obsolescence.

Albeit Value-Added Services running over legacy Circuit-Switched Core Networks will endure for at least a decade (especially in developing countries), the unavoidable requirement to adapting to whole new paradigms like Service Oriented Architecture and the Internet of Things, tightly coupled with the onset of new technologies and communication protocols like SIP and Diameter based on all-IP Packet Switched Core Networks, set the basis and led us to this research and development work.

### Aims

As vast as the topics are as depicted in the background of this work, it becomes imperative to limit the scope of this study according to a master's degree in research and development. Hence, the general objective of this MSc thesis is

enabling Value-Added Services deployment within heterogeneous networks environments, by developing transparent messaging and positioning mechanisms according to international standardization organizations, with focus on 3GPP/LTE technical specifications.

In order to comply with the general aim outlined previously, the following specific objectives are described next:

1. Select an open source workspace which includes a service delivery platform, as well as network testing/simulation frameworks, with capabilities for the construction of solutions for heterogeneous telecommunication networks.
2. Develop an Application Programmable Interface (API) and complement network resources adapters/enablers for providing alternatives to current omissions either of the chosen platform or supplement emerging specifications for seamless messaging and location services either for legacy or next generation networks.
3. Develop a prototype and configure the testing/simulating framework to validate services using evaluation methods according to DESMET [100] methodology.

## Methods

As previously stated, this section details the activities required by the project. As the latter is organized under the «Logical Framework Approach» [92], certain products are described for each of the specific objectives.

Concerning the first specific objective, i.e.: «select an open source workspace which includes a service delivery platform, as well as network testing/simulation frameworks, with capabilities for the construction of solutions for heterogeneous telecommunication networks», the programmed activities for its accomplishment follow:

- According to publications in indexed journals and/or conferences related to the objective, investigate the workspaces (service delivery platforms for the deployment of services and networks test/simulation environments) that led to success cases aligned with the overall objective.
- Investigate advantages and disadvantages, contributions and breaches of the existing workspaces related with the overall objective.
- Investigate viability of deployment within and industrial environment in terms of reliability, robustness, scalability, flexibility, etc.
- According with the objectives and architecture of University of Cauca GIT «Telco 2.0» or NGN/IMS laboratory assembly project, study the feasibility of integrating into it the selected service delivery platform.

Concerning the second specific objective, i.e.: «develop an Application Programmable Interface (API) and complement network resources adapters/enablers for providing alternatives to current omissions either of the chosen platform or supplement emerging specifications for seamless messaging and location services either for legacy or next generation networks», the programmed activities for its accomplishment follow:

- Deploy the chosen open source service delivery platform and validate the correct operation of its capabilities, enablers and resource adaptors for MAP, SIP and Diameter.
- Establish communication channels relevant to the provision of support and collaboration with the developers of the selected platform.
- Develop an Application Programmable Interface for supporting provision of Location Based Services independently of the triggering channel.
- Implementation of additions to resource adaptors and APIs for the selected service delivery platform according to 3GPP/LTE standards for messaging and location services, and thus allowing transparency to the user of the service across heterogeneous mobile access networks.

Concerning the third specific objective, i.e.: «develop a prototype and configure the testing/simulating framework to validate services using evaluation methods

according to DESMET methodology», the programmed activities for its accomplishment follow:

- Produce a controlled testing environment of services by the deployment of the needed network architecture for the operation/simulation of value-added services for mobile telephony. At the beginning of the project, University of Cauca GIT «Telco 2.0» or NGN/IMS laboratory assembly ongoing initiative and open source frameworks like the ones referenced in [53, 83-90] comprise the basis for building a simulation environment of core network entities/interfaces according to the general objective of the project. Finally, TeleStax testing environment tools and QA methodologies detailed in [122] were used.
- Design and develop convergent services according to described motivational scenarios needs, namely:
  - Trigger LCS through Diameter extensions according to [43-45] for NGN or via MAP operations [22] via multiple means like Mobile Originated (MO) or Network Initiated (NI) USSD/USSI or REST Web Services;
- Selection of one or more of the proposed DESMET methods for the evaluation of extensions and services developed according to the following criteria:
  - API and selected framework expansion compliance for USSD and LCS support, respectively over SIP and Diameter, according to 3GPP TS 24.390 [42] y 29.172/3 [44-45] guidelines.
  - Applicability and/or feasibility for the expansion and/or migration of VAS services among industrial premises.
  - Feasibility and quality of impact analysis for the motivational scenarios concerning the project, i.e., Republic of Colombia Ministry of Information Technologies and Telecommunications «National Network of Emergency Telecommunications for LTE» and Commission for the Regulations of Communications «Guidelines for Mobile Financial Services», United States of America National Emergency Number Association (NENA) Next Generation 911 (NGG911) or Peruvian «Stalker Law».
- Liaise with R&D teams involved in similar projects that may contribute to the platform's development and validation processes.



## Results

As a result of the activities carried out, the following products have been accomplished, available to the entire telecommunication software development community, given the open source nature of the chosen framework.

- «RestComm Geolocation API», first open Source geolocation API for interaction with mobile networks and retrieval of location information under cellular radio access networks and/or WiFi. The design and framework chosen for the API's development allow adding value to new or pre-existing telecommunication services across heterogeneous networks. In other words, gathered mobile location information might be retrieved autonomously or triggered by asynchronous events from messaging services, voice, etc., independently of the underlying network infrastructure. Please refer to chapter 7 for detailed highlights of the API according to the final evaluation.
- Release of the first Open Source GMLC according to international standardization groups such as 3GPP/LTE and OMA for the retrieval of location information under any radio access network. Please refer to chapter 7 for detailed highlights of «RestComm GMLC» according to the final evaluation.
- Only Open Source development of Diameter based SL<sub>h</sub> y SL<sub>g</sub> interfaces for LTE location services according to 3GPP TS 29.172/29.173 [44-45].
- RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.

## Conclusions

Following a very ambitious work initiative and after narrowing the scope of the MSc thesis to achievable objectives, the general and specific objectives have been accomplished within an ideal framework, given the adoption of TeleStax, the company behind the open source project of communications more widespread globally, i.e. RestComm (successor of Mobicents).

It is important to note that the implementation of the project entailed a very arduous work, given the historical context during which it was carried out. Unlike in previous decades, mobile telecommunications operators are no longer in the advantageous conditions of the pre-OTT («Over-The-Top») era. It is thus that any innovation initiative that involves costs is much more difficult to move forward than before, during which operator's revenues were such that even those R&D projects that involved uncertainties comprised accomplishment chances.

IP telephony and aforementioned OTT's irruption have dramatically changed the rules of the game. Given that the objectives of this work clearly address deployment of solutions within mobile telecommunications networks and specifically, mobile network operators, the task became practically a chimera. Ironically, this context far from becoming a «show-stopper», in the long run ended up benefiting it. Motives will be explained following.

Large telecommunications organizations, whether operators or vendors, have had to adjust to current massive technological paradigm shifts era. Furthermore, during an unfavorable financial context, these big players listed in the stock exchange are beginning to look favorably to Open Source initiatives, already proven successful (e.g. Linux, JBoss, Hadoop, Cloudera, etc.). TeleStax product portfolio belong to that category. Hence, mounting the project under this framework provides access to mobile network operators, something almost impossible from an academic-only initiative. Having said that, it also comprised a huge challenge incorporating a non-

planned functionality in the roadmap of a company like TeleStax, whose prime objective is establishing as the leading Cloud VoIP broker. A laborious presentation very well received at the Restconn 2015 event [E10-E16], pathed the way in this regard.

During the design and development of this work, both the Open Source community supported by TeleStax (born after the emergence of the Mobicents project), as well as TeleStax certified partners brought up appreciated contributions. It was thus that the work was vetted with valuable contributions from these sources and also for this reason it was possible to acquire an evaluation of some outstanding professionals related to this project's area of knowledge. Furthermore, an idea given birth under an academic environment, regardless of the field experience of this work author, ends up becoming also an industrial endeavour. Finally, given the fact that the project fits within an Open Source framework supported by a vibrant community, the space for academic projects related to the area of knowledge in question is wide open. Hence, the scope for the continuity of this work is established either from the industrial or academic perspective.

From an industrial point of view, the products of this work are being considered by Mobile Network Operators for the integration among their networks, which obviously satisfies the expectations created at initial stage of this labour. Some of these initiatives are being treated directly with the operators, while other ones through certified partners (which is evidenced throughout the qualitative surveys used as evaluation method according to DESMET methodology). Likewise, the products of this work are framed under an MFS (Mobile Financial System) project for development countries in Africa and Latin America, where real-time retrieval of location information resolves several matters for revenue assurance and fraud departments, as well as for marketing involved in the deployment of promotions by geographic zones. Similarly, location reports triggered by events as introduced in this work, allow customer tracking so as to alerting and/or preventing inappropriate use of promotional messaging.

Additionally, given the role of the author of this work under TeleStax enterprise and his academic bonds, as advices in the previous paragraph, it is intended to promote and assist research and development projects in the academic field under

related areas of knowledge. This obviously involves University of Cauca or any academic institution willing to participate. National projects like the ones mentioned under the motivational scenarios (RNTE and SFM) perfectly matches this kind of academic-enterprise collaboration initiatives. Other projects in which University of Cauca has been decisively involved like «Tucan3G» [E17-E18], could smoothly adjust too, for instance, for the provisioning of real time location information for emergency medical assistance throughout distant rural areas. In the same manner, conversations are being maintained with the «Illinois Institute of Technology» R&D members related to projects for next generation emergency services (NG911) for the National Emergency Number Association (NENA) in the United States of America [105], more specifically, with those involved in the project for «Dispatchable Indoor Location for Mobile Phones Calling for Emergency Services» [139].

Concluding, as a result of this work, carried out under the framework of the most important and globally active open source telecommunications software platform (as can be verified in [E19-E20]), besides from accomplishing the planned objectives, the seed has been sowed for the continuity and expansion of the project, both at an industrial and academic level. Refer to Chapter 7 of this document for more details on future work.

**Keywords:** HetNets, Location Based Services, MAP, Diameter, SIP.

# Content

<b>PÁGINA DE ACEPTACIÓN .....</b>	<b>III</b>
<b>ACKNOWLEDGEMENT PAGE.....</b>	<b>V</b>
<b>RESUMEN ESTRUCTURADO .....</b>	<b>VII</b>
<b>STRUCTURED ABSTRACT .....</b>	<b>XVII</b>
<b>CONTENT .....</b>	<b>XXV</b>
<b>ILLUSTRATIONS INDEX .....</b>	<b>XXXV</b>
<b>TABLES INDEX .....</b>	<b>XLIII</b>
<b>GLOSSARY.....</b>	<b>XLV</b>
<b>CHAPTER 1 .....</b>	<b>1</b>
<b>1 INTRODUCTION .....</b>	<b>1</b>
1.1 OVERALL CONTEXT .....	1
1.2 DEFINITION OF THE PROBLEM .....	2
1.3 MOTIVATIONAL SCENARIOS .....	3
1.4 SCOPE .....	4
1.5 CONTRIBUTIONS AND RESULTS.....	5
1.6 MONOGRAPH STRUCTURE .....	5
<b>CHAPTER 2 .....</b>	<b>7</b>
<b>2 STATE OF THE ART .....</b>	<b>7</b>
2.1 CONCEPTUAL BASIS .....	7
2.2 RELATED WORKS .....	19

2.3	LOCATION SERVICES IN CELLULAR NETWORKS .....	26
2.4	USSD AND USSI .....	32
<b>CHAPTER 3.....</b>		<b>35</b>
<b>3 OPEN SOURCE FRAMEWORK: RESTCOMM.....</b>		<b>35</b>
3.1	INTRODUCTION .....	35
3.2	FEATURES .....	38
3.3	USSD AND SMSC GATEWAYS.....	39
3.4	OTHER COMPONENTS .....	42
3.5	CONCLUSION .....	44
<b>CHAPTER 4.....</b>		<b>45</b>
<b>4 RESTCOMM GEOLOCATION API.....</b>		<b>45</b>
4.1	GEOLOCATION RESOURCE .....	48
4.1.1	<i>Geolocation Resource URI</i> .....	48
4.1.2	<i>Geolocation Resource Properties</i> .....	49
4.1.3	<i>Supported Operations</i> .....	54
4.2	IMMEDIATE GEOLOCATION.....	55
4.2.1	<i>Immediate Geolocation URI</i> .....	55
4.2.2	<i>Immediate Geolocation supported operations</i> .....	55
4.2.3	<i>Immediate Geolocation list of required parameters</i> .....	56
4.2.4	<i>Immediate type of Geolocation examples</i> .....	56
4.2.4.1	Immediate Geolocation of a specific IP device associated to a User; Partial and Successful answers, whole Status Callback cycle example.....	56
4.2.4.2	Geolocation of a specific Mobile device associated to a phone number; response including geographic coordinates .....	59
4.2.4.3	Geolocation of a specific Mobile Device associated to a phone number; no geographic coordinates included in response .....	60
4.2.4.4	Geolocation of a specific IP device associated to a user: Failed execution response .....	61
4.2.4.5	Geolocation update of a previously failed request .....	61
4.2.4.6	Gathering information of a specific previously satisfactory created Geolocation Request.....	62
4.2.4.7	Rejected Immediate Geolocation request.....	63
4.3	NOTIFICATION GEOLOCATION .....	64
4.3.1	<i>Notification Geolocation URI</i> .....	64
4.3.2	<i>Notification Geolocation supported operations</i> .....	64
4.3.3	<i>Notification Geolocation list of required parameters</i> .....	65
4.3.4	<i>Notification type of Geolocation examples</i> .....	66

4.3.4.1	Geolocation of a specific IP device when it enters a 1km range of a specific Geolocation - Partial and Successful answers, whole Status Callback cycle example .....	66
4.3.4.2	Geolocation of a specific IP device when it enters a 1km range of a specific Geolocation: Unauthorized Answer .....	69
4.3.4.3	Geolocation of a specific IP device when it enters a 1km range of a specific Geolocation: Rejected Answer	70
4.3.4.4	Geolocation of a specific IP device when it enters a 200 metres range of a specific Geolocation: Success Answer	70
4.3.4.5	Geolocation of a specific IP device when it enters a 300m range of a specific Geolocation with High Accuracy: Success Answer .....	71
4.3.4.6	Update previous Geolocation request for a specific IP device when it exits a 300m range of a specific Geolocation: Success Answer .....	73
4.3.4.7	Retrieve information of a specific previously satisfactory created Geolocation Request .....	74
4.3.4.8	Stop Notifications of a specific previously created Geolocation Request .....	75
4.4	CELLULAR GEOLOCATION SIGNAL FLOWS .....	75
4.5	IP GEOLOCATION SIGNAL FLOW .....	77
4.6	GEOLOCATION STATUS CALLBACKS SEQUENCE DIAGRAM .....	78
4.7	RESTCOMM CELLULAR GEOLOCATION CONFIGURATION .....	79
4.8	RESTCOMM RCML .....	80
4.8.1	<i>RCML verb Geolocation</i> .....	80
4.8.1.1	Geolocation verb attributes .....	80
4.8.1.2	Request Parameters .....	81
4.8.1.3	Nesting .....	82
4.8.1.3.1	Notification noun attributes .....	82
4.8.1.4	RCML Geolocation verb examples .....	84
4.8.2	<i>RestComm Visual Designer and Geolocation verb</i> .....	85
<b>CHAPTER 5</b>	.....	<b>87</b>
<b>5 RESTCOMM GMLC</b>	.....	<b>87</b>
5.1	GMLC SUMMARY AND ENHANCEMENTS INTRODUCED .....	87
5.2	HTTP PROCEDURES FOR LOCATION REQUESTS .....	95
<b>CHAPTER 6</b>	.....	<b>109</b>
<b>6 EVALUATION</b>	.....	<b>109</b>
6.1	EVALUATION METHOD ANALYSIS .....	109
6.2	QUALITATIVE SURVEYS .....	112
<b>CHAPTER 7</b>	.....	<b>117</b>

<b>7</b>	<b>CONCLUSIONS AND FUTURE WORK .....</b>	<b>117</b>
7.1	RESULTS .....	117
7.2	FUTURE WORK .....	119
	<b>BIBLIOGRAPHY .....</b>	<b>121</b>
	<b>EXTENDED BIBLIOGRAPHY .....</b>	<b>139</b>
	<b>ANNEX A.....</b>	<b>143</b>
<b>A</b>	<b>SIGNALING SYSTEM N°7 .....</b>	<b>143</b>
A.1	INTRODUCTION TO SS7 .....	143
A.1.1	<i>History</i> .....	143
A.1.2	<i>Types of signaling</i> .....	145
A.1.2.1	Channel Associated Signaling (CAS) .....	145
A.1.2.2	Common Channel Signaling (CCS) .....	146
A.2	SIGNALING SYSTEM N°7 NETWORK ENTITIES .....	147
A.2.1	<i>Signaling Modes</i> .....	153
A.2.1.1	Associated Signaling Mode .....	153
A.2.1.2	Non-Associated Signaling Mode.....	154
A.2.1.3	Quasi-Associated Signaling Mode .....	154
A.2.2	<i>Links and Linksets</i> .....	155
A.2.3	<i>Route and Routesets</i> .....	158
A.3	SS7 PROTOCOL STACK.....	160
A.3.1	<i>Message Transfer Part (MTP)</i> .....	160
A.3.1.1	MTP Layer 1: Signaling Data Physical Layer.....	161
A.3.1.2	MTP Layer 2: Signaling Link Layer .....	162
A.3.1.2.1	Signaling Units .....	163
A.3.1.2.1.1	Message Signal Unit (MSU) .....	163
A.3.1.2.1.2	Fill In Signal Unit (FISU) .....	164
A.3.1.2.1.3	Link Status Unit .....	164
A.3.1.2.1.4	Error Correction .....	166
A.3.1.3	MTP Layer 3: Signaling Network Layer .....	168
A.3.1.3.1	MTPL3 Treatment of Signaling Messages functions .....	170
A.3.1.3.1.1.1	Routing Label (ITU-T).....	171
A.3.1.3.1.1.2	Service Information Octet .....	172
A.3.1.3.2	MTPL3 Network Management of the Signaling Network functions .....	173
A.3.1.4	Integrated Services for Digital Network User Part (ISUP).....	174
A.3.1.4.1	ISUP Message Structure .....	178
A.3.1.4.2	ISUP Call Signaling .....	181



A.3.1.4.2.1	Initial Address Message (IAM).....	182
A.3.1.4.2.2	Address Complete Message (ACM).....	184
A.3.1.4.2.3	Answer Message (ANM).....	185
A.3.1.4.2.4	Release Message (REL).....	186
A.3.1.4.2.5	Release Complete Message (RLC).....	187
A.3.2	<i>Signaling Connection Control Part (SCCP)</i> .....	188
A.3.2.1.1	Routing based on SSN/DPC.....	189
A.3.2.1.2	Routing based on Global Title Translation.....	190
A.3.2.1.3	SCCP Management.....	192
A.3.2.1.4	SCCP Message Structure.....	192
A.3.2.1.4.1	SCCP Calling/Called Party Address.....	194
A.3.2.1.4.1.1	Address Indicator (AI).....	196
A.3.2.1.4.2	Signaling Point Code (SPC).....	199
A.3.2.1.4.3	Sub System Number (SSN).....	199
A.3.2.1.4.4	Translation Type (TT).....	200
A.3.2.1.4.5	Encoding Scheme (ES).....	201
A.3.2.1.4.6	Numbering Plan.....	201
A.3.2.1.4.7	Nature of Address Indicator.....	202
A.3.2.1.4.8	Global Title Address Information (ITU-T).....	203
A.3.2.1.4.9	Global Title Format and Address Information (ANSI).....	203
A.3.3	<i>Transaction Capabilities Application Part (TCAP)</i> .....	204
A.3.3.1	TCAP Component States and State Transitions.....	206
A.3.3.2	TCAP Message Structure.....	209
A.3.3.2.1.1	Transactional Sublayer (ITU-T).....	211
A.3.3.2.1.2	Transaction Portion (ANSI).....	213
A.3.3.2.1.3	Component Sublayer (ITU-T).....	214
A.3.3.2.1.4	Component Portion (ANSI).....	214
A.3.3.2.1.5	TCAP Message Types.....	215
A.3.3.3	TCAP Dialog.....	217
A.3.3.3.1	TCAP Dialog types.....	217
A.3.3.3.2	TCAP Dialog Unit.....	218
A.3.3.3.2.1.1	Application Context Name.....	219
A.3.3.3.2.1.2	Protocol Version.....	220
A.3.3.3.2.1.3	User Info.....	220
A.3.3.3.2.1.4	Result.....	221
A.3.3.3.2.1.5	Result Resource Diagnostic.....	221
A.3.3.3.2.1.6	Abort Source.....	221
A.3.3.3.2.1.7	Dialog Abort.....	221
A.3.4	<i>Mobile Application Part (MAP)</i> .....	221
A.3.4.1	MAP Service Primitives and Dialogs.....	222
A.3.4.1.1	MAP Service Primitives' Sequence Rules.....	226
A.3.4.1.1.1	Opening.....	226
A.3.4.1.1.2	Continuing.....	227
A.3.4.1.1.3	Closing.....	227

A.3.4.1.1.4	Aborting .....	228
A.3.4.1.1.5	General rules for mapping of MAP services onto TCAP .....	228
A.3.4.1.1.6	MAP Service primitives' parameters .....	231
A.3.4.1.1.6.1	Invoke Id .....	231
A.3.4.1.1.6.2	Linked Id .....	233
A.3.4.1.1.6.3	Provider Error .....	234
A.3.4.1.1.6.4	User Error .....	234
A.3.4.1.1.6.5	Operation Codes .....	234
A.3.5	<i>Customised Applications for Mobile Enhanced Logic (CAMEL)</i> .....	240
A.3.5.1	CAP Definitions and Architecture .....	246
A.3.5.1.1	CAP Operations .....	248
A.3.5.2	CAMEL Call Control .....	252
A.3.5.2.1	Detection Points (DP) .....	252
A.3.5.2.2	Basic Call State Model (BCSM) .....	253
A.3.5.2.2.1	Originated BCSM (O-BCSM) .....	253
A.3.5.2.2.2	Terminated BCSM (T-BCSM) .....	257
A.3.5.3	CAMEL GPRS Control .....	259
A.3.5.3.1	GPRS Attach .....	261
A.3.5.3.2	GPRS Attach/Detach State Model .....	262
A.3.5.3.3	PDP Context (PDPc) .....	263
A.3.5.3.3.1	GPRS PDP Context State Model .....	266
A.3.5.3.4	GTP Tunnel .....	267
A.3.5.3.5	GPRS Control Scenarios .....	268
A.3.5.3.5.1	Scenario 1 in GPRS Control .....	268
A.3.5.3.5.2	Scenario 2 in GPRS Control .....	269
A.3.5.3.5.2.1	Sequence control for GPRS Control scenarios .....	270
A.3.5.3.6	GPRS Finite State Machine .....	271
A.3.5.3.7	Implicitly disarming rules for Detection Points in CAMEL GPRS Control .....	273
A.3.5.3.8	TCAP Segmentation .....	274
A.3.5.4	CAMEL SMS Control .....	277
A.3.6	<i>Introduction to Signaling Transport for SS7 over IP (SIGTRAN)</i> .....	278
A.3.6.1	SIGTRAN Architecture Entities .....	279
A.3.6.2	SIGTRAN protocol stack .....	281
A.3.6.2.1	Stream Control Transport Protocol (SCTP) .....	281
A.3.6.2.1.1	SCTP Association .....	282
A.3.6.2.1.2	Multi-homing .....	284
A.3.6.2.2	Multi-streaming .....	285
A.3.6.2.3	SCTP datagram structure .....	286
A.3.6.2.4	MTP3 User Adaptation Layer (M3UA) .....	291
A.3.6.2.5	M3UA datagram structure .....	293

**ANNEX B..... 299**

**B GLOBAL SYSTEM FOR MOBILE (GSM) ..... 299**

B.1	INTRODUCTION.....	299
B.2	GSM NETWORK ARCHITECTURE .....	300
<i>B.2.1</i>	<i>Base Station Subsystem (BSS)</i> .....	<i>300</i>
B.2.1.1	GSM Logical Channels .....	302
<i>B.2.2</i>	<i>Network Subsystem (NSS)</i> .....	<i>305</i>
<i>B.2.3</i>	<i>Network Management Subsystem (NMS)</i> .....	<i>307</i>
B.2.3.1	GSM Registration, Authentication and Location procedure .....	308
B.2.3.2	Basic Call Establishment.....	310
B.3	GPRS/EDGE NETWORK ARCHITECTURE.....	311
<b>ANNEX C.....</b>		<b>315</b>
<b>C UMTS AND NGN .....</b>		<b>315</b>
C.1	INTRODUCTION TO UMTS.....	315
<i>C.1.1</i>	<i>3GPP UMTS R99 and R4 main characteristics</i> .....	<i>317</i>
C.1.1.1.1	Wideband Code Division Multiple Access (WCDMA) .....	318
<i>C.1.2</i>	<i>UMTS Releases 6 Network Architecture</i> .....	<i>320</i>
C.1.2.1	UTRAN.....	321
C.1.2.2	UMTS Circuit-Switched Core Network .....	321
C.1.2.3	IP Multimedia Subsystem (IMS) .....	324
C.1.2.3.1	IMS Components.....	324
C.1.2.3.2	IMS Communication Protocols.....	332
C.2	BRIEF INTRODUCTION TO NGN .....	333
<i>C.2.1</i>	<i>NGN Layers</i> .....	<i>335</i>
C.2.1.1	Session Border Controller (SBC) .....	336
<b>ANNEX D.....</b>		<b>339</b>
<b>D LONG TERM EVOLUTION (LTE) .....</b>		<b>339</b>
D.1	INTRODUCTION TO LTE .....	339
D.2	NETWORK ARCHITECTURE .....	343
<i>D.2.1</i>	<i>Evolved Packet Core (EPC)</i> .....	<i>343</i>
<i>D.2.2</i>	<i>Evolved UMTS Radio Access Network (E-UTRAN)</i> .....	<i>346</i>
<i>D.2.3</i>	<i>Network Architecture Interfaces Roles</i> .....	<i>348</i>
<i>D.2.4</i>	<i>LTE User Plane Protocol Stack</i> .....	<i>349</i>
<i>D.2.5</i>	<i>LTE Control Plane Protocol Stack</i> .....	<i>351</i>
<i>D.2.6</i>	<i>NAS Procedures</i> .....	<i>353</i>
<i>D.2.7</i>	<i>High Level Control Plane Protocols</i> .....	<i>355</i>
D.3	VOLTE AND LTE SERVICES.....	357

D.4	LTE-ADVANCED .....	360
<b>ANNEX E .....</b>		<b>363</b>
<b>E VOICE OVER IP OVERVIEW .....</b>		<b>363</b>
E.1	INTRODUCTION TO VOIP .....	363
E.2	BASIC COMPONENTS OF A VOIP NETWORK .....	365
E.3	VOIP ARCHITECTURES .....	367
E.3.1	<i>Centralized Architecture</i> .....	368
E.3.2	<i>Distributed Architecture</i> .....	368
E.4	CONTROL AND USER PLANES IN VOIP NETWORKS .....	368
E.4.1	<i>VoIP Control Plane Protocols</i> .....	369
E.4.1.1	Session Initiation Protocol (SIP) .....	371
E.4.1.1.1	SIP Architecture and Agents .....	373
E.4.1.1.2	SIP Transactions and User Agents roles .....	376
E.4.1.1.3	SIP in the IMS .....	382
E.4.1.1.4	SIP Addresses .....	384
E.4.1.1.5	SIP Messages .....	385
E.4.1.1.5.1	SIP Messages Header Fields .....	395
E.4.1.1.5.2	SIP Message Body .....	397
E.4.1.1.5.3	SIP Methods Examples .....	397
E.4.1.1.5.3.1	SIP REGISTER .....	397
E.4.1.1.5.3.2	SIP INVITE .....	398
E.4.1.1.5.3.3	SIP CANCEL .....	401
E.4.1.1.5.3.4	SIP PRACK .....	404
E.4.1.1.5.3.5	SIP SUBSCRIBE / NOTIFY .....	406
E.4.1.1.5.3.6	SIP PUBLISH .....	407
E.4.1.1.5.3.7	SIP UPDATE .....	408
E.4.1.1.5.3.8	SIP MESSAGE .....	409
E.4.1.1.5.3.9	SIP REFER .....	409
E.4.1.1.6	USSD over SIP (USSI) .....	413
E.4.2	<i>VoIP User Plane Protocols</i> .....	424
E.4.2.1	Real-time Transport Protocol (RTP) .....	424
E.4.2.1.1	RTP Packet Structure .....	426
E.4.2.2	RTP Control Protocol (RTCP) .....	429
E.4.2.2.1	RTCP Packet Structure .....	431
E.4.2.3	Security for RTP/RTCP: SRTP .....	432
E.5	BRIEF INTRODUCTION TO WEBRTC .....	433
E.5.1	<i>SIP over WebSockets for WebRTC</i> .....	435
<b>ANNEX F .....</b>		<b>437</b>

<b>F</b>	<b>DIAMETER</b>	<b>437</b>
F.1	INTRODUCTION TO DIAMETER	437
F.2	DIAMETER BASE DEFINITIONS AND GENERALITIES	437
F.2.1	<i>Diameter Transport</i>	438
F.2.2	<i>Diameter Functional Entities</i>	439
F.2.3	<i>Diameter Resource Identifiers</i>	441
F.2.4	<i>Diameter Connections and Sessions</i>	442
F.3	DIAMETER MESSAGE STRUCTURE	443
F.3.1	<i>Diameter AVP structure</i>	447
F.4	DIAMETER BASE PROTOCOL COMMANDS	450
F.4.1	<i>Abort-Session-Request / Abort-Session-Answer (ASR/ASA)</i>	451
F.4.2	<i>Device-Watchdog-Request / Device-Watchdog-Answer (DWR/DWA)</i>	451
F.4.3	<i>Disconnect-Peer-Request/Disconnect-Peer-Answer (DPR/DPA)</i>	452
F.4.4	<i>Accounting-Request / Accounting-Answer (ACR/ACA)</i>	452
F.4.5	<i>Capabilities-Exchange-Request/Answer (CER/CEA)</i>	453
F.4.6	<i>Re-Authentication-Request/Answer (RAR/RAA)</i>	453
F.4.7	<i>Session-Termination-Request/Answer (STR/STA)</i>	453
F.5	DIAMETER IN THE IMS AND LTE	453
F.5.1	<i>Authentication and Authorization in the IMS</i>	455
F.5.1.1	<i>User-Authorization-Request/Answer (UAR/UAA)</i>	456
F.5.1.2	<i>Multimedia-Auth-Request/Answer (MAR/MAA)</i>	457
F.5.1.3	<i>Server-Assignment-Request/Answer (SAR/SAA)</i>	457
F.5.1.4	<i>Location Information Request/Answer (LIR/LIA)</i>	458
F.5.2	<i>Policy and Charging Control (PCC) in the IMS</i>	460
F.5.2.1.1	<i>PCC and Offline Charging Architecture in the IMS</i>	464
F.5.2.1.2	<i>PCC and Online Charging Architecture in the IMS</i>	468
F.5.3	<i>Diameter AAA in VoLTE</i>	472
F.6	INTRODUCTION TO RESTCOMM jDIAMETER	474
F.6.1	<i>SLh and SLg jDiameter implementation</i>	479
F.6.1.1	<i>SLh test example</i>	479
F.6.1.2	<i>SLg test example</i>	480
<b>ANNEX G</b>		<b>485</b>
<b>G</b>	<b>EVALUATION</b>	<b>485</b>
G.1	QUALITATIVE SURVEYS GUIDELINES	485
G.2	QUALITATIVE SURVEY OF JEAN DERUELLE	490
G.3	QUALITATIVE SURVEY OF ANDREW EROSS	495
G.4	QUALITATIVE SURVEY OF MARCELO ARANIBAR	500

G.5 QUALITATIVE SURVEY OF JAMES BODY..... 504  
G.6 QUALITATIVE SURVEY OF JULIO REY ..... 509

## Illustrations Index

FIGURE 2.1. WORLDWIDE WIRELESS TECHNOLOGIES AND STANDARDS EVOLUTION. ....	15
FIGURE 2.2. TELCO SERVICE FLOW WITH INTEGRATED SOA BACKPLANE. ....	17
FIGURE 2.3. TELCO BUSINESS ROLES EXAMPLE BEFORE AND AFTER SOA. (SOURCE: JOURNAL OF SOFTWARE AND SYSTEMS DEVELOPMENT [118]). ....	18
FIGURE 2.4. LOCATION SERVICES ARCHITECTURE IN GSM, GPRS/EDGE AND UMTS ACCORDING TO 3GPP. ....	27
FIGURE 2.5. CELL GLOBAL IDENTITY ASSEMBLY AS FOR 3GPP TS 23.003. ....	28
FIGURE 2.6. LOCATION SERVICES ARCHITECTURE IN LTE ACCORDING TO 3GPP/LTE AND OMA. ....	29
FIGURE 2.7. USSD CALL FLOW EXAMPLE OF PREPAID SUBSCRIBER TOPUP. ....	34
FIGURE 3.1. SDP INTEGRATED INTO A TELCO ORGANIZATIONAL ENVIRONMENT UNDER THE SOA PARADIGM. ....	36
FIGURE 3.2. TELESTAX RESTCOMM COMMUNICATION PLATFORM ARCHITECTURE BASED ON MOBICENTS. ....	37
FIGURE 3.3. TELESTAX' RESTCOMM OPPORTUNITY OFFER TO CSPs (SOURCE: ALAN QUAYLE [120]). ....	39
FIGURE 3.4. SIGNAL FLOW EXAMPLE OF MOBILE ORIGINATED USSD SESSION ESTABLISHED WITH THIRD PARTY APPLICATION THROUGHOUT TELESTAX ENTERPRISE RESTCOMM ACROSS SS7 AND IP-BASED NETWORKS (ANNEX E PROVIDES A TRACE FOR SUCH EXAMPLE). ....	40
FIGURE 3.5. SIGNAL FLOW EXAMPLE OF MOBILE ORIGINATED SMS DELIVERY TO THIRD PARTY APPLICATION THROUGHOUT RESTCOMM ACROSS SS7 AND IP-BASED NETWORKS. ....	41
FIGURE 3.6. TELESTAX ENTERPRISE RESTCOMM, SMSC AND USSD GATEWAYS INTERNETWORKING AMONG HETEROGENEOUS NETWORKS. ....	42
FIGURE 3.7. LTE VIDEO CALL VIA RESTCOMM IOS/ANDROID SDK. ....	43
FIGURE 3.8. TELESTAX' COMMUNICATION PLATFORMS INTEGRATED TO MNO CORE NETWORKS FROM GSM TO LTE. ....	44
FIGURE 4.1. RESTCOMM API'S SIMPLE ACCESS DIAGRAM. ....	46
FIGURE 4.2. RESTCOMM GEOLOCATION API REST API ENDPOINT STRUCTURE. ....	47
FIGURE 4.3. IMMEDIATE GEOLOCATION SEQUENCE DIAGRAM OF RESTCOMM AND GMLC IN GSM NETWORKS. ....	76
FIGURE 4.4. NOTIFICATION TYPE OF GEOLOCATION IN UMTS/3G CELLULAR NETWORKS. ....	76
FIGURE 4.5. NOTIFICATION TYPE OF GEOLOCATION IN 4G/LTE CELLULAR NETWORKS. ....	77
FIGURE 4.6. IMMEDIATE IP GEOLOCATION SEQUENCE DIAGRAM OF RESTCOMM WITH OLYMPUS CLIENTS AND RESTCOMM MOBILE/WEB SDKS. ....	78
FIGURE 4.7. GEOLOCATION STATUS CALLBACKS SEQUENCE DIAGRAM. ....	79
FIGURE 4.8. EXAMPLE OF GEOLOCATION VERB USAGE IN RVD USSD PROJECT (IMMEDIATE). ....	86
FIGURE 4.9 EXAMPLE OF GEOLOCATION VERB USAGE IN RVD USSD PROJECT (NOTIFICATION). ....	86
FIGURE 5.1. RESTCOMM GMLC IN HETEROGENEOUS NETWORKS ENVIRONMENTS. ....	89
FIGURE 5.2. TELESTAX ENTERPRISE/RESTCOMM GMLC LCS SIGNAL FLOW IN UMTS. ....	91
FIGURE 5.3. TELESTAX ENTERPRISE/RESTCOMM GMLC LCS SIGNAL FLOW IN LTE. ....	92

FIGURE 5.4. RESTCOMM GMLC SOFTWARE ARCHITECTURE AND INTERFACES.....	94
FIGURE 5.5. EXAMPLE OF SIMPLE GMLC GSM LOCATION SERVICE TRIGGERED BY HTTP GET.....	95
FIGURE 5.6. GMLC PERFORMANCE TEST: CPU AND MEMORY CONSUMPTION STATISTICS [129].....	107
FIGURE 5.7. GMLC PERFORMANCE TEST: HTTP SAMPLES STATISTICS [129].....	108
FIGURE A - 1. CHANNEL ASSOCIATED SIGNALING (CAS).....	145
FIGURE A - 2. COMMON CHANNEL SIGNALING (CCS).....	146
FIGURE A - 3. COMMON CHANNEL SIGNALING PATH BETWEEN SIGNALING SWITCHING POINTS.....	147
FIGURE A - 4. SERVICE SWITCHING POINTS CONTROL AND USER PLANES PATHS.....	148
FIGURE A - 5. NETWORK ARRANGEMENT OF LOCAL AND TANDEM EXCHANGES.....	149
FIGURE A - 6. NETWORK ARRANGEMENT OF STPs AND SSPs.....	150
FIGURE A - 7. SCP'S CONNECTIONS TO STPs FOR GTT.....	151
FIGURE A - 8. INTELLIGENT NETWORK ENTITIES INTERNETWORKING.....	152
FIGURE A - 9. ASSOCIATED SIGNALING MODE.....	153
FIGURE A - 10. NON-ASSOCIATED SIGNALING MODE.....	154
FIGURE A - 11. QUASI ASSOCIATED SIGNALING MODE.....	155
FIGURE A - 12. TYPE OF SIGNALING LINKS IN SS7.....	156
FIGURE A - 13. LINK AND LINKSET ARRANGE BETWEEN THREE SPs.....	157
FIGURE A - 14. ROUTE AND ROUTESETS AND THEIR RESPECTIVE LINKSETS BETWEEN FOUR SPs.....	159
FIGURE A - 15. SS7 PROTOCOL STACK VERSUS OSI LAYER MODEL.....	160
FIGURE A - 16. SIGNALING UNIT PATH BETWEEN MTP USERS.....	161
FIGURE A - 17. SIGNALING DATA LINKS AND E1 FRAME STRUCTURE.....	162
FIGURE A - 18. SS7 SIGNALING UNITS.....	163
FIGURE A - 19. LSSU STRUCTURE.....	165
FIGURE A - 20. LSSU MESSAGE EXCHANGE FOR INITIAL LINK ALIGNMENT.....	166
FIGURE A - 21. EXAMPLE OF MESSAGE EXCHANGE ACCORDING TO THE MSU BASIC ERROR CONTROL METHOD IN MTPL2.....	167
FIGURE A - 22. SIGNALING UNIT ASSEMBLY.....	168
FIGURE A - 23. MSU: ROUTING LABEL AND SERVICE INDICATOR OCTET (ITU-T).....	169
FIGURE A - 24. MSU: ROUTING LABEL AND SERVICE INDICATOR OCTET (ANSI).....	170
FIGURE A - 25. MTPL3 TREATMENT OF SIGNALING MESSAGES FUNCTIONS.....	170
FIGURE A - 26. MTPL3 SIGNALING NETWORK MANAGEMENT FUNCTIONS.....	173
FIGURE A - 27. SIGNALING NETWORK MANAGEMENT MSU FORMAT.....	174
FIGURE A - 28. ISDN USER-NETWORK ACCESS REFERENCE CONFIGURATION.....	175
FIGURE A - 29. ISDN INFRASTRUCTURES/ACCESSES.....	176
FIGURE A - 30. SIGNALING STAGES BETWEEN ISND USERS.....	177
FIGURE A - 31. ISUP MESSAGE STRUCTURE EMBEDDED IN MSU'S SIF.....	179
FIGURE A - 32. ISUP SIGNALING TRANSPORT VIA E1 BETWEEN LOCAL EXCHANGES (LE) SUBSCRIBERS, EITHER FOR ASSOCIATED OR QUASI/NON-ASSOCIATED SIGNALING MODES.....	180
FIGURE A - 33. ISUP MESSAGE ENCAPSULATION IN SS7 MSU ACCORDING TO ITU-T.....	180
FIGURE A - 34. UNCONDITIONAL CALL FORWARDING (UCF) SIGNALING EXAMPLE.....	182



FIGURE A - 35. ISUP IAM MESSAGE STRUCTURE ACCORDING TO ITU-T. ....	183
FIGURE A - 36. ISUP ACM MESSAGE STRUCTURE ACCORDING TO ITU-T. ....	184
FIGURE A - 37. ISUP ANM MESSAGE STRUCTURE ACCORDING TO ITU-T. ....	185
FIGURE A - 38. ISUP REL MESSAGE STRUCTURE ACCORDING TO ITU-T. ....	186
FIGURE A - 39. ISUP RLC MESSAGE STRUCTURE ACCORDING TO ITU-T. ....	187
FIGURE A - 40. SCCP PLACEMENT IN SS7 PROTOCOL STACK. ....	188
FIGURE A - 41. SERVICE CONTROL POINTS WITH ONE OR SEVERAL SSN. ....	189
FIGURE A - 42. GLOBAL TITLE TRANSLATION EXAMPLE FOR 0800 DIALING. ....	190
FIGURE A - 43. IN/CAMEL SERVICE CALL FLOW BETWEEN SSP AND SCP WITH GLOBAL TITLE TRANSLATION AT THE STP. ....	191
FIGURE A - 44. SCCP MESSAGE STRUCTURE AND ENCAPSULATION IN SS7 MSU (ITU-T). ....	193
FIGURE A - 45. SCCP CALLING/CALLED PARTY ADDRESS STRUCTURE (ITU-T). ....	195
FIGURE A - 46. SCCP CALLING/CALLED PARTY ADDRESS STRUCTURE (ANSI). ....	195
FIGURE A - 47 SCCP ADDRESS INDICATOR. ....	196
FIGURE A - 48. SCCP CAPA/CdPA SIGNALING POINT CODE FIELD (ITU-T). ....	199
FIGURE A - 49. SCCP CALLING/CALLED PARTY ADDRESS SUB SYSTEM NUMBER FIELD (ITU-T). ....	199
FIGURE A - 50. SCCP GLOBAL TITLE ADDRESS INFORMATION (ITU-T). ....	203
FIGURE A - 51. SCCP GLOBAL TITLE FORMAT AND ADDRESS INFORMATION (ANSI). ....	203
FIGURE A - 52. TCAP PLACEMENT IN SIGTRAN AND PURE SS7 PROTOCOL STACK. ....	204
FIGURE A - 53 CLASS 1 OPERATIONS STATE TRANSITION DIAGRAM. ....	207
FIGURE A - 54. CLASS 2 OPERATIONS STATE TRANSITION DIAGRAM. ....	207
FIGURE A - 55. CLASS 3 OPERATIONS STATE TRANSITION DIAGRAM. ....	208
FIGURE A - 56. CLASS 4 OPERATIONS STATE TRANSITION DIAGRAM. ....	208
FIGURE A - 57. TCAP MESSAGE STRUCTURE AND ENCAPSULATION IN SS7 MSU (ITU-T). ....	209
FIGURE A - 58. TCAP MESSAGE GENERAL STRUCTURE. ....	210
FIGURE A - 59. TCAP MESSAGE INFORMATION ELEMENT STRUCTURE. ....	211
FIGURE A - 60. STRUCTURED TCAP DIALOG EXAMPLE BETWEEN SIGNALING POINTS. ....	218
FIGURE A - 61. MAP SERVICE PRIMITIVE (USSD) EXAMPLE EMBEDDED WITHIN AN SS7 MSU. ....	223
FIGURE A - 62. MAP OPENING SEQUENCE. ....	226
FIGURE A - 63. MAP CONTINUING SEQUENCE. ....	227
FIGURE A - 64. MAP CLOSING SEQUENCE. ....	227
FIGURE A - 65. MAP ABORTING SEQUENCE. ....	228
FIGURE A - 66. STRUCTURED MAP SERVICE (SMS) «INVOKE ID» VALUES EXAMPLE. ....	232
FIGURE A - 67. UNSTRUCTURED MAP SERVICE (USSD) «INVOKE ID» VALUES EXAMPLE. ....	233
FIGURE A - 68. CAMEL FUNCTIONS, ENTITIES/NODES AND INTERFACES IN SS7 BASED CORE NETWORKS. ....	244
FIGURE A - 69. CAP PROTOCOL ARCHITECTURE. ....	247
FIGURE A - 70. BASIC COMPONENTS IDENTIFIED AT THE BCSM. ....	253
FIGURE A - 71. ORIGINATING BCSM FOR CAMEL [23]. ....	254
FIGURE A - 72. CAMEL O-BCSM CALL FLOW EXAMPLE (CALLING PARTY RUNS OUT OF CREDIT). ....	256
FIGURE A - 73. ORIGINATING BCSM FOR CAMEL [23]. ....	257
FIGURE A - 74 CAMEL T-BCSM EXAMPLE (CALLING PARTY DISCONNECTS). ....	259

FIGURE A - 75. GPRS CAMEL CONTROL STACK DIAGRAM.....	260
FIGURE A - 76. GPRS ATTACH PROCEDURE. ....	262
FIGURE A - 77. GPRS ATTACH/DETACH STATE MODEL (3GPP TS 23.060). ....	263
FIGURE A - 78. PDPc ESTABLISHMENT FOR GERAN TYPE OF ACCESS.....	264
FIGURE A - 79. PDPc ESTABLISHMENT FOR UTRAN TYPE OF ACCESS.....	265
FIGURE A - 80. GPRS PDP CONTEXT STATE MODEL.....	267
FIGURE A - 81. GTP TUNNEL EXAMPLES FOR GERAN OR UTRAN TYPE OF ACCESS. ....	268
FIGURE A - 82. GPRS CONTROL: SCENARIO 1 EXAMPLE.....	269
FIGURE A - 83. GPRS CONTROL: SCENARIO 2 EXAMPLE.....	269
FIGURE A - 84. EXAMPLE OF SEQUENTIAL INVOCATION OF GPRS CAMEL CONTROL SCENARIOS 1 AND 2. ....	270
FIGURE A - 85. RULES FOR REPORTING OF EVENTS RELATED TO PDP CONTEXTS ACCORDING TO GPRS CONTROL SCENARIOS 1 AND 2. .....	271
FIGURE A - 86. GPRS FSM SERVICE LOGIC EXAMPLE AS FOR SCENARIO 1. ....	272
FIGURE A - 87. GPRS FSM SERVICE LOGIC EXAMPLE AS FOR SCENARIO 2. ....	272
FIGURE A - 88. GPRS FSM TRANSITIONS.....	273
FIGURE A - 89. TCAP SEGMENTATION MECHANISM FROM THE GPRS FSM PERSPECTIVE. ....	275
FIGURE A - 90. EXAMPLE OF TCAP DIALOG SEGMENTATION FOR CAMEL GPRS CONTROL.....	276
FIGURE A - 91. NETWORK ARCHITECTURE ENTITIES AND INTERFACES FOR CAMEL SMS CONTROL.....	277
FIGURE A - 92. MO SMS CAMEL CONTROL SIGNAL FLOW. ....	278
FIGURE A - 93. SCTP ASSOCIATION EXAMPLE FOR IP ASPs. ....	283
FIGURE A - 94. SCTP HANDSHAKE EXAMPLE. ....	283
FIGURE A - 95. SIGTRAN MULTI-HOMING. ....	284
FIGURE A - 96. SCTP PACKET RETRANSMISSION EXAMPLE IN MULTI-HOMING SETUP. ....	285
FIGURE A - 97. MULTI-STREAMING WITHIN AN SCTP ASSOCIATION.....	286
FIGURE A - 98. SCTP DATAGRAM STRUCTURE. ....	287
FIGURE A - 99. SCTP DATAGRAM DATA CHUNK WIRESHARK TRACE EXAMPLE. ....	291
FIGURE A - 100. SIGNALING GATEWAY BASED ON SCTP/M3UA. ....	292
FIGURE A - 101. M3UA DATAGRAM STRUCTURE.....	293
FIGURE A - 102. M3UA DATA MESSAGE STRUCTURE.....	297
FIGURE A - 103. M3UA MESSAGE WIRESHARK TRACE EXAMPLE. ....	298
FIGURE B - 1. MOBILE SUBSCRIPTIONS BY TECHNOLOGY [10]. ....	300
FIGURE B - 2. IMSI STRUCTURE. ....	301
FIGURE B - 3. MSISDN STRUCTURE. ....	302
FIGURE B - 4. FDMA/TDMA STRUCTURE OF GSM [14].....	303
FIGURE B - 5. GSM LOGICAL CHANNEL STRUCTURE [E1]. ....	305
FIGURE B - 6. IMEI AND IMEISV STRUCTURE. ....	307
FIGURE B - 7. GSM NETWORK SUBSYSTEMS AND MAIN ENTITIES OVERVIEW. ....	308
FIGURE B - 8. GSM REGISTRATION, AUTHENTICATION AND LOCATION UPDATE PROCEDURES. ....	309
FIGURE B - 9. SIMPLE MOBILE ORIGINATED/TERMINATED CALL ESTABLISHMENT IN GSM. ....	310

FIGURE B - 10. GMS AND GPRS/EDGE BASIC NETWORK OVERVIEW. ....	314
FIGURE C - 1. 3GPP ORGANIZATION STRUCTURE. ....	316
FIGURE C - 2. WCDMA SPREAD SPECTRUM TRANSMISSION AND RECEPTION WITH RAKE RECEIVER. ....	319
FIGURE C - 3. QPSK AND 8PSK MODULATION SCHEME CONSTELLATIONS. ....	320
FIGURE C - 4. MSCS CONTROL PLANE USER-NETWORK AND NETWORK-NETWORK SIGNALING. ....	322
FIGURE C - 5. MSCS – CS-MGW SIGNALING. ....	323
FIGURE C - 6. USER PLANE USER-NETWORK SIGNALING AT THE CS-MGW EITHER RTP/UDP/IP OR AAL2/ATM BASED. ....	324
FIGURE C - 7. HSS LOGIC FUNCTIONS AND INTERFACES WITH ENTITIES OF THE CS AND PS CNS AS FOR 3GPP TS 23.002. ....	326
FIGURE C - 8. PSTN GATEWAY PROTOCOL MAPPING. ....	330
FIGURE C - 9. UMTS-IMS CALL FLOW. ....	331
FIGURE C - 10. GSM/GPRS/UMTS/IMS INTERNETWORKING. ....	332
FIGURE D - 1. OFDMA DOWNLINK CHANNEL PROGRAMMING IN TIME AND FREQUENCY DOMAINS IN LTE (DAHLMAN ET AL [8]). ...	340
FIGURE D - 2. 16QAM AND 64QAM CONSTELLATIONS. ....	341
FIGURE D - 3. LTE/LTE-ADVANCED EVOLUTION AS PER 3GPP RELEASES 8 TO 10 (DAHLMAN ET AL [8]). ....	342
FIGURE D - 4. EPS (LTE+SAE) INTERNETWORKING. ....	345
FIGURE D - 5. LTE E-UTRAN INTERFACES. ....	347
FIGURE D - 6. LTE INTERFACES ROLES. ....	348
FIGURE D - 7. LTE USER PLANE PROTOCOL STACK. ....	349
FIGURE D - 8. LTE CONTROL PLANE PROTOCOL STACK. ....	352
FIGURE D - 9. LTE INITIAL ATTACH PROCEDURE. ....	354
FIGURE D - 10. LTE TRACKING AREA UPDATE. ....	355
FIGURE D - 11. LTE DEDICATED BEARER ACTIVATION PROCEDURE. ....	357
FIGURE D - 12. VOLGA INTERNETWORKING. ....	358
FIGURE D - 13. VOLTE TRAVERSING E-UTRAN, EPC AND IMS (VOIMS). ....	360
FIGURE E - 1. NGN ARCHITECTURE VIEW ACCORDING TO ITU-T Y-1202. ....	335
FIGURE E - 2. NGN LAYER MODEL ACCORDING TO [145]. ....	336
FIGURE E - 3. INTERNETWORKING GSM/GPRS/UMTS/IMS/LTE. ....	346
FIGURE E - 4. VOIP BASIC COMPONENTS. ....	366
FIGURE E - 5. BASIC IMS INTERNETWORKING WITH CS CN LIKE THE PSTN OR PLMN. ....	367
FIGURE E - 6. CONTROL AND USER PLANES IN VOIP. ....	369
FIGURE E - 7. BASIC CALL CONTROL VIA SIP OVER IP NETWORKS OVERVIEW. ....	372
FIGURE E - 8. EXAMPLES OF SIP USER AGENTS. ....	373
FIGURE E - 9. SIP ARCHITECTURE COMPONENTS AND AGENTS. ....	374
FIGURE E - 10. SIP SERVERS INVOLVED IN MULTIMEDIA COMMUNICATIONS CONTROLLED BY SIP. ....	376
FIGURE E - 11. SIP TRAPEZOID. ....	377
FIGURE E - 12. SIP CALL ESTABLISHMENT TRANSACTION SCENARIOS. ....	378

FIGURE E - 13. EXAMPLE OF SIP UA ROLES DURING SIP SESSION TRANSACTIONS. ....	379
FIGURE E - 14. SIP INVITE CLIENT/SERVER TRANSACTION STATE MODELS. ....	381
FIGURE E - 15. SIP REQUEST MESSAGE STRUCTURE EXAMPLE. ....	386
FIGURE E - 16. SIP RESPONSE MESSAGE STRUCTURE EXAMPLE. ....	387
FIGURE E - 17. SIP END-TO-END VERSUS HOP-BY-HOP MESSAGES. ....	389
FIGURE E - 18. SIP REGISTER EXAMPLE. ....	398
FIGURE E - 19. CONVENTIONAL SIP CALL ESTABLISHMENT WITH PROXIES. ....	399
FIGURE E - 20. SIP CALL ESTABLISHMENT: THE PROXY MODE. ....	400
FIGURE E - 21. SIP CALL ESTABLISHMENT: THE REDIRECT MODE. ....	401
FIGURE E - 22. SIP CANCEL METHOD NORMAL PROCEDURE EXAMPLE. ....	402
FIGURE E - 23. CANCEL METHOD. MESSAGE CROSS EXAMPLE WHEN A FINAL RESPONSE WAS PREVIOUSLY RECEIVED, DERIVING IN TERMINATION VIA BYE. ....	403
FIGURE E - 24. SIMPLE PRACK METHOD EXAMPLE DURING A SIP INVITE TRANSACTION. ....	404
FIGURE E - 25. PRACK METHOD EXAMPLE DURING A SIP INVITE TRANSACTION WITH A PACKET LOSS. ....	405
FIGURE E - 26. SIP SUBSCRIBE / NOTIFY NORMAL TRANSACTION EXAMPLE. ....	406
FIGURE E - 27. SIP PUBLISH / NOTIFY METHODS EXAMPLE. ....	407
FIGURE E - 28. SIP UPDATE METHOD EXAMPLE FOR QoS UPDATE DURING SIP INVITE TRANSACTION. ....	408
FIGURE E - 29. SIP MESSAGE METHOD EXAMPLE. ....	409
FIGURE E - 30. SIP REFER METHOD EXAMPLE FOR CALL TRANSFERENCE. ....	410
FIGURE E - 31. SIP REFER METHOD EXAMPLE FOR WEB PAGE RETRIEVAL THROUGH HTTP GET. ....	411
FIGURE E - 32. SIP REFER METHOD EXAMPLE FOR CALL TRANSFER WITH RELEASE FROM THE USER TARGET OF THE TRANSFER. ....	412
FIGURE E - 33. TELESTAX ENTERPRISE USSD GATEWAY BETWEEN LEGACY SS7 AND NEXT GENERATION NETWORKS CONVEYING USSD MESSAGES EITHER OVER MAP OR SIP CORRESPONDINGLY. ....	413
FIGURE E - 34. RTP PACKET EXAMPLE TRANSPORTING AN AUDIO SAMPLE VIA UDP. ....	426
FIGURE E - 35. RTP PACKET HEADER. ....	429
FIGURE E - 36. THIS FIGURE SHOWS HOW RTCP MAPPINGS PERFORM INTER-MEDIA SYNCHRONIZATION [34]. ....	430
FIGURE E - 37. RTCP COMPOUND PACKET STRUCTURE [SOURCE: IETF RFC 3550]. ....	432
FIGURE E - 38. AUTHENTICATED AND ENCRYPTED RTP PACKET SECTIONS [34]. ....	433
FIGURE E - 39. WEBRTC PEER-TO-PEER COMMUNICATION MAIN COMPONENTS, CONTROL AND USER PLANES. ....	434
FIGURE E - 40. WEBRTC ARCHITECTURE. ....	435
FIGURE E - 41. WEBRTC CALL ESTABLISHMENT VIA SIP POST HTTP WEBSOCKET UPGRADE. ....	436
FIGURE F - 1. EXAMPLE OF DIAMETER BASE PROTOCOL AND SOME EXTENSIONS. ....	438
FIGURE F - 2. DIAMETER CONNECTIONS AND SESSIONS. ....	442
FIGURE F - 3. DIAMETER MESSAGE STRUCTURE. ....	446
FIGURE F - 4. DIAMETER AVP STRUCTURE. ....	447
FIGURE F - 5. AUTHENTICATION AND AUTHORIZATION IN THE IMS ON FIRST SIP REGISTER. ....	458
FIGURE F - 6. USE OF DIAMETER LIR/LIA IN THE IMS SIP INVITE REQUEST WITH NO «ROUTE» HEADER INCLUDED. ....	459
FIGURE F - 7. PCC ARCHITECTURE IN THE IMS. ....	460
FIGURE F - 8. PUSH MODE PCC CALL FLOW ON INCOMING SIP INVITE REQUEST. ....	461

FIGURE F - 9. PULL MODE PCC CALL FLOW ON INCOMING SIP INVITE REQUEST. ....	462
FIGURE F - 10. PUSH MODE PCC CALL FLOW ON OUTGOING SIP INVITE REQUEST. ....	463
FIGURE F - 11. PULL MODE PCC CALL FLOW ON OUTGOING SIP INVITE REQUEST. ....	464
FIGURE F - 12. PCC IN THE IMS: OFFLINE CHARGING ARCHITECTURE. ....	465
FIGURE F - 13. PCC IN THE IMS: SESSION ESTABLISHING CALL FLOW WITH OFFLINE CHARGING. ....	467
FIGURE F - 14. PCC IN THE IMS: ONLINE CHARGING ARCHITECTURE. ....	468
FIGURE F - 15. IMMEDIATE EVENT CHARGING (IEC) FOR ONLINE CHARGING IN THE IMS. ....	469
FIGURE F - 16. EVENT CHARGING WITH UNIT RESERVATION (ECUR) FOR ONLINE CHARGING IN THE IMS. ....	470
FIGURE F - 17. SESSION CHARGING WITH UNIT RESERVATION (SCUR) FOR ONLINE CHARGING IN THE IMS. ....	471
FIGURE F - 18. VOLTE CALL FLOW FIRST STAGE: SESSION ESTABLISHMENT AND AAA. ....	472
FIGURE F - 19. VOLTE CALL FLOW FIRST STAGE: SESSION UPDATE AND ONLINE BILLING REPORT. ....	473
FIGURE F - 20. RESTCOMM JDIAMETER BASIC ARCHITECTURE. ....	474
FIGURE F - 21. RESTCOMM JDIAMETER STACK SL <sub>H/G</sub> APPLICATION SESSION CONTROL BY CORRESPONDING SESSION FACTORY. ....	475
FIGURE F - 22. RESTCOMM JDIAMETER MUX ARCHITECTURE. ....	476
FIGURE F - 23. JAIN SLEE FRAMEWORK AND JDIAMETER PROTOCOL STACK WITHIN RESTCOMM MIDDLEWARE CORE NETWORK ENTITIES' ARCHITECTURE AND EXTERNAL AGENTS OR PERIPHERAL NETWORK NODES. ....	478
FIGURE F - 24. JDIAMETER SL <sub>H</sub> RIR EXAMPLE (SAMPLE CONTAINING ALL AVPS EXECUTED). ....	480
FIGURE F - 25. JDIAMETER SL <sub>H</sub> RIA EXAMPLE (SAMPLE CONTAINING ALL AVPS EXECUTED). ....	480
FIGURE F - 26. JDIAMETER SL <sub>G</sub> PLR EXAMPLE (SAMPLE CONTAINING ALL AVPS EXECUTED). ....	481
FIGURE F - 27. JDIAMETER SL <sub>G</sub> PLA EXAMPLE (SAMPLE CONTAINING ALL AVPS EXECUTED). ....	482
FIGURE F - 28. JDIAMETER SL <sub>G</sub> LRR EXAMPLE (SAMPLE CONTAINING ALL AVPS EXECUTED). ....	483
FIGURE F - 29. JDIAMETER SL <sub>G</sub> LRA EXAMPLE (SAMPLE CONTAINING ALL AVPS EXECUTED). ....	483



## Tables Index

TABLE 2.1. TECHNICAL ASPECTS OF MAIN 2G MOBILE COMMUNICATION SYSTEMS. ....	10
TABLE 2.2. RAN POSITIONING METHODS COMPARISON. ....	31
TABLE 4.1. RESTCOMM GEOLOCATION API RESOURCE PROPERTIES. ....	54
TABLE 4.2. IMMEDIATE GEOLOCATION LIST OF REQUIRED PARAMETERS. ....	56
TABLE 4.3. GEOLOCATION RCML VERB ATTRIBUTES. ....	80
TABLE 4.4. RESTCOMM GEOLOCATION RCML REQUEST PARAMETERS. ....	81
TABLE 4.5. NOTIFICATION NOUN ATTRIBUTES. ....	82
TABLE 6.1. SUMMARY OF THE EVALUATION SURVEY RESULTS. ....	115
TABLE A - 1. SS7 LINK TYPES.....	157
TABLE A - 2. STATUS INDICATOR POSSIBLE VALUES DESCRIPTION. ....	165
TABLE A - 3. MTPL3 USER ACCORDING TO SERVICE INDICATOR VALUE. ....	172
TABLE A - 4. BASIC CALL ISUP MESSAGES. ....	181
TABLE A - 5. SCCP MANAGEMENT MESSAGES. ....	192
TABLE A - 6. SCCP GLOBAL TITLE INDICATOR FIELD VALUES MEANING. ....	197
TABLE A - 7. SCCP ADDRESS INDICATOR VALUE EXAMPLES AS FOR ITU-T.....	198
TABLE A - 8. NETWORK ENTITIES SSN VALUES.....	200
TABLE A - 9. SCCP CAPA/CdPA TRANSLATION TYPE VALUES MEANING. ....	200
TABLE A - 10. SCCP CAPA/CdPA ENCODING SCHEME VALUES MEANING. ....	201
TABLE A - 11. SCCP CAPA/CdPA NUMBERING PLAN VALUES MEANING. ....	202
TABLE A - 12. SCCP CAPA/CdPA NATURE OF ADDRESS INDICATOR VALUES MEANING. ....	202
TABLE A - 13. PRIMITIVES FOR TCAP TR (ITU). ....	212
TABLE A - 14. TYPES AND PARAMETERS FOR EACH MAP SERVICE PRIMITIVE. ....	226
TABLE A - 15. MAPPING OF MAP COMMON SERVICES ONTO TCAP SERVICES [22]. ....	229
TABLE A - 16. MAPPING OF TC SERVICES ONTO MAP COMMON SERVICE [22]. ....	230
TABLE A - 17. MAPPING OF MAP USER SPECIFIC SERVICES ONTO TC SERVICES [22]. ....	230
TABLE A - 18. MAPPING OF TC SERVICES ONTO MAP USER SPECIFIC SERVICES [22]. ....	231
TABLE A - 19. MAP OPERATION CODES AND APPLICATION CONTEXT NAMES. ....	239
TABLE A - 20. CAP OPERATIONS FOR CAMEL CALL, SMS AND GPRS CONTROL. ....	251
TABLE A - 21. IMPLICIT DISARMED DPs IN THE O-BCSM. ....	255
TABLE A - 22. IMPLICIT DISARMED DPs IN THE T-BCSM.....	258
TABLE A - 23. INFORMATION ELEMENTS FOR GPRS CONTROL. ....	261
TABLE A - 24. PDPC INFORMATION ELEMENTS FOR GPRS CONTROL. ....	266

# XLIV

TABLE A - 25. GPRS/SS7 FSM STATES DESCRIPTION.....	273
TABLE A - 26. IMPLICITLY DISARMED DP RULES FOR GPRS CAMEL SCENARIO 2.....	274
TABLE A - 27. IMPLICITLY DISARMED DP RULES FOR GPRS CAMEL SCENARIO 2.....	274
TABLE B - 1. UPDATE OF THE GSM NETWORK FOR GPRS DEPLOYMENT.....	312
TABLE D - 1. LTE INITIAL RELEASES MAIN CHARACTERISTICS.....	342
TABLE E - 1. SDP ACRONYMS TYPES AND MEANINGS.....	388
TABLE E - 2. SIP METHODS MAIN CHARACTERISTICS.....	394
TABLE E - 3. SIP STATUS CODE RANGES AND THEIR MEANINGS.....	395
TABLE E - 4. DIFFERENCES BETWEEN CLASSIC VOIP AND WEBRTC.....	433
TABLE F - 1. DIAMETER BASE PROTOCOL COMMANDS.....	451
TABLE F - 2. DIAMETER COMMANDS FOR AUTHENTICATION AND AUTHORIZATION IN THE IMS.....	456



## Glossary

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
5G-PPP	5G Infrastructure Public Private Partnership
AAA	Authentication, Authorization and Accounting
ABMF	Account Balance Management Function
ACN	Application Context Name
ADC	Administration Centre
ADSL	Asymmetric Digital Subscriber Line
AECID	Adaptive Enhanced Cell Identity
A-GNSS	Assisted Global Navigation Satellite System
ANSI	American National Standards Institute
AoA	Angle of Arrival
AP	Access Point
API	Application Programmable Interface
APN	Access Point Name
ARIB	Association of Radio Industries and Business
AS	Application Server or Access Stratum
ASP	Application Server Process
ASR	Automatic Speech Recognition
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
AVP	Attribute Value Pairs
BCSM	Basic Call State Model
BGCF	Breakout Gateway Control Function
BICC	Bearer Independent Call Control
BSC	Base Station Controller
BSS	Business Support Systems
BSS	Base Station Subsystem

BSSAP	BSS Application Part
BTS	Base Transceiver Station
C7	Common Channel Signaling System No. 7
CA	Carrier Aggregation
CAMEL	Customised Applications for Mobile Enhanced Logic
CAP	CAMEL Application Part
CaPA	Calling Party Address
CAS	Channel Associated Signaling
CCF	Call Control Function
CCITT	Consultative Committee for International Telephony and Telegraphy
CCS	Common Channel Signaling
CCSA	China Communications Standards Association
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CdPA	Called Party Address
CDR	Call Detail Record
CEO	Chief Executive Officer
CEPT	Conference of Postal and Telecommunications Administrations
CGF	Charging Gateway Function
CI	Cell Identity
CIC	Circuit Identification Code
CIDR	Classless Inter-Domain Routing
CRC	Comisión de Regulación de Comunicaciones
CRC	Cyclic Redundancy Check
CS CN	Circuit-Switched Core Network
CSCF	Call Session Control Function
CSFB	Circuit Switch Fall-Back
CSFB	Circuit-Switched Fall Back
CSI	CAMEL Subscription Information
CS-MGW	Circuit Switched Multimedia Gateway
CSP	Communication Service Provider
CSRC	Contributing Source
CTF	Charging Trigger Function
CTO	Chief Technology Officer

DCCA	Diameter Credit Control Application
DCCP	Datagram Congestion Control Protocol
DeNB	Donor eNB
DP	Detection Point
DPC	Destination Point Code
DSL	Digital Subscriber Line
DTLS	Datagram Transport Layer Security
DTMF	Dual Tone Multi Frequency
EBCF	Event Based Charging Function
ECID	Enhanced Cell Identity
ECUR	Event Charging with Unit Reservation
EDGE	Enhanced Data rates for GSM Evolution
EIA-41	Electronic Industries Alliance
EIR	Equipment Identity Register
EJB	Enterprise Java Bean
ELP	EPC Location Protocol
EMM	EPS Mobility Management
eNB	Evolved Node B
E-OTD	Enhanced Observed Time Difference
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ES	Encoding Scheme
ESM	EPS Session Management
E-SMLC	Evolved-Serving Mobile Location Centre
eTOM	Enhanced TOM
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EVDO	Evolution Data Only/Optimized
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FISU	Fill In Signaling Unit
FOSS	Free and Open Source Software
FSM	Finite State Machine

## XLVIII

FTP	File Transfer Protocol
GCI	Global Cell Identity
GERAN	GPRS EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GLONASS	Global Navigation Satellite System
GMCS	Gateway MSC
GMLC	Gateway Mobile Location Centre
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile
GSMA	GSM Association
gsmSCF	GSM Service Control Function
gsmSRF	GSM Specialized Resource Function
gsmSSF	GSM SSF
GT	Global Title
GTP	GPRS Tunneling Protocol
GTT	Global Title Translation
HARQ	Hybrid Automatic Repeat reQuest
HFC	Hybrid Fiber-Coaxial
HLR	Home Location Register
H-PLMN	Home PLMN
HSDPA	High-Speed Downlink Packet Access
HSPA	High-Speed Packet Access
HSS	Home Subscriber Server
HSUPA	High-Speed Uplink Packet Access
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IBCF	Interconnection Border Control Function
ICIC	Inter-Cell Interference Coordination
I-CSCF	Interrogating CSCF
ICT	Information and Communication Technologies
IEC	Immediate Event Charging
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IF	Interworking Function
IIT	Illinois Institute of Technology
IM	Instant Messaging
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMS GWF	IMS Gateway Function
IMSI	International Mobile Subscriber Identity
IMT-2000	International Mobile Telecommunications-2000
IN	Intelligent Networks
INAP	Intelligent Network Application Protocol
IP	Internet Protocol or Intelligent Peripheral or Internetworking Protocol
IPSP	Internet Protocol Signaling Point
ISC	IMS Service Control
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
IT	Information Technologies
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
JAIN SLEE	Java APIs for Integrated Networks Service Logic Execution Environment
Kc	Cryptography Key
Ki	Authentication Key
LAC	Location Area Code
LAN	Local Area Network
LBS	Location Based Services
LCS	Location Services
LE	Local Exchange
LRA	Location Report Answer
LRR	Location Report Request
LSSU	Link Status Unit
LTE	Long Term Evolution
M3UA	MTP3 User Adaptation Layer
MAC	Medium Access Control

## L

MAP	Mobile Application Part
MAP ATI	MAP Any Time Interrogation
MAP PSL	MAP Provide Subscriber Location
MAP SLR	MAP Subscriber Location Report
MAP SRforLCS	MAP Send Routing Information for Location Services
MBMS	Multimedia Broadcast Multicast Service
MCC	Mobile Country Code
MFS	Mobile Financial Services
MGC	Media Gateway Controller
MGCF	Media Gateway Control Function
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MIME	Multipurpose Internet Mail Extensions
MIMO	Multiple Input Multiple Output
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
MLP	Mobile Location Protocol
MME	Mobility Management Entity
MMI	Man-Machine Interface
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MNO	Mobile Network Operator
MNP	Mobile Number Portability
MNP	Mobile Number Portability
MO	Mobile Originated
MPLS	Multi Protocol Label Switching
MS	Mobile Station
MSC	Mobile Switching Centre
MSCS	Mobile Switching Centre Server
MSIN	Mobile Subscriber Identity Number
MSISDN	Mobile Station International Subscriber Directory Number
MSU	Message Signaling Unit
MTP	Message Transfer Part
MUX	Multiplexer
NAI	Nature of Address Information
NAS	Non Access Stratum or Network Access Server

NAT	Network Address Translation
NB	Node B
NENA	National Emergency National Association
NFV	Network Function Virtualization
NG911	Next Generation 911
NGN	Next Generation Networks
NGOSS	New Generation Operations Systems and Software
NI	Network Initiated
NMC	Network Management Center
NMS	Network Management System
NNI	Network-to-Network Interface
NP	Numbering Plan
NSS	Network Switching Subsystem
NTP	Network Time Protocol
OCS	Online Charging System
OFCS	Offline Charging System
OFDMA	Orthogonal Frequency Division Multiple Access
OMA	Open Mobile Alliance
OMC	Operation and Maintenance Center
OPC	Originating Point Code
OS	Operating System
OSS	Operations Support Systems
OTDOA	Observed Time Difference Of Arrival
OTT	Over the Top
P2P	Peer to Peer
PC	Point Code
PCC	Policy and Charging Control
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCM	Pulse Code Modulation
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network or Public Switched Data Network
PDPc	Packet Data Protocol Context

P-GW	Packet Data Network Gateway
PLA	Provide Location Answer
PLMN	Public Land Mobile Network
PLR	Provide Location Request
POJO	Plain Old Java Object
PS CN	Packet-Switched Core Network
PSAP	Public Service Answering Point
PSTN	Public Switched Telephone Network
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quad Phase Shift Keying
R&D	Research and Development
RA	Resource Adaptor
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RANAP	Radio Access Network Application Part
REST	Representational State Transfer
RF	Rating Function
RFC	Request For Comments
RIA	Routing Information Answer
RIR	Routing Information Request
RLC	Radio Link Control
RNC	Radio Network Controller
RNTE	Red Nacional de Telecomunicaciones de Emergencia
RRC	Radio Resource Control
RRM	Radio Resource Management
RSTD	Reference Signal Time Difference
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
RVD	RestComm Visual Designer
SAS	Stand-Alone SMLC
SBB	Service Building Block
SBC	Session Border Controller
SBCF	Session Based Charging Function



SCCP	Signaling Connection Control Part
SCE	Service Creation Environment
SCP	Service Control Point
S-CSCF	Serving CSCF
SC-TDMA	Single Carrier TDMA
SCTP	Stream Control Transmission Protocol
SCUR	Session Charging with Unit Reservation
SDCCH	Stand-Alone Dedicated Control Channel
SDF	Service Data Function
SDH	Synchronous Digital Hierarchy
SDK	Software Development Kit
SDN	Software Defined Networking
SDP	Service Data Point
SDP	Session Description Protocol
SEE	Service Execution Environment
SET	SUPL Enabled Terminal
SGSN	Serving GPRS Support Node
SGW	Signaling Gateway
S-GW	Serving Gateway
SIF	Service Information Field
SIGTRAN	Signaling Transport
SIM	Subscriber Identity Module
SIO	Service Information Octet
SIP	Session Initiation Protocol
SIP-AS	SIP Application Server
SLF	Subscriber Location Function
SLIA	Standard Location Immediate Answer
SLIR	Standard Location Immediate Request
SLIREP	Standard Location Immediate Report
SLP	SUPL Location Platform
SMLC	Serving Mobile Location Centre
SMP	Service Management Point
SMPP	Short Message Peer-to-Peer
SMS	Short Messages Service
SMS IWMSC	SMS Inter Working MSC

LIV

SMSC	Short Message Service Centre
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SON	Self-Optimizing Network
SP	Signaling Point
SPC	Signaling Point Code
SPR	Subscriber Profile Repository
SRF	Specialized Resource Function
SRF	Specialized Resource Function
SRNS	Serving Radio Network Subsystem
SRTTP	Secure RTP
SRVCC	Single Radio Voice Call Continuity
SRVCC	Single Radio Voice Call Continuity
SS7	Signalling System N° 7
SSF	Service Switching Function
SSN	Subsystem Number
SSP	Service Switching Point
SSRC	Synchronization Source
STP	Signaling Transfer Point
SU	Signaling Unit
SUPL	Secure User Plane Location
TA	Timing Advance
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TDOA	Time Difference Of Arrival
TD-SCDMA	Time Division Synchronous Code Division Multiple Access
TE	Tandem Exchange
TIA	Telecommunications Industry Association
TISPAN	Telecoms and Internet converged Services and Protocols for Advanced Networks
TLS	Transport Layer Security
TMN	Telecommunications Management Network
TMSI	Temporal Mobile Subscriber Identity
TOM	Telecom Operations Map

TR	Technical Report
TRAU	Transcoder and Rate Adaptation Unit
TS	Technical Specification
TS	Timeslot
TT	Translation Type
TTA	Telecommunications Technology Association
TTS	Telecommunications Technology Committee
TTS	Text-to-Speech
UE	User Equipment
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data
USSI	USSD for the IMS
UTDOA	Uplink Time Difference Of Arrival
UTRAN	UMTS Terrestrial Radio Access Network
VANC	VoLGA Access Network Controller
VAS	Value-Added Services
VLR	Visitor Location Register
VMSC	Visited MSC
VoIMS	Voice over IMS
VoIP	Voice over IP
VoLGA	Voice over LTE Generic Access
VoLTE	Voice over LTE
V-PLMN	Visited PLMN
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WDM	Wavelength Division Multiplexing
WebRTC	Web Real-Time Communication
WGS84	World Geodetic System 1984
WiMAX	Worldwide Interoperability for Microwave Access

LVI

WLAN

Wireless LAN

XML

eXtensible Markup Language

XMLRPC

XML Remote Procedure Call

# Chapter 1

## 1 Introduction

### 1.1 Overall context

In the meantime Communication Service Providers (CSPs) such as Mobile Network Operators (MNOs) are currently under the vortex arising from paradigm shifts imposed by the omnipresence of the Internet, mobile telecommunications technologies evolution continues its migration from incompatible networks, protocols and communication devices, towards a global convergence of multimedia services in which big corporations, engineers, universities and researchers partake under recommendations and standards of international organizations, i.e. ITU-T/R/D [1], 3GPP/LTE [2], IETF [3], IEEE [4], OMA [5], GSMA [6], TM Forum [7] and 5G-PPP [104].

All of these standards and technologies concomitance continues its permanent evolution mainly due to a growing demand of more complex and bandwidth demanding Value-Added Services (VAS). Ongoing deployment of mobile telecommunications ultimate architecture known as LTE/LTE-Advanced [8-9], comprising network topologies and services uniquely based on the Internet Protocol (IP), will turn obsolete traditional telephony Circuit-Switched Core Networks over which digital mobile communications have thrived since its inception. Adoption of new trends based on IP-based architectures, such as Voice over LTE or «VoLTE» [79-80] emerges as a liability for MNOs to stand up against unavoidable revenue loss due to Over the Top (OTT) applications.

Notwithstanding, as can be deduced from the latest Ericsson Mobility Report [10] and ITU's ICT Facts and Figures report [11], an all IP scenario is far from becoming a worldwide reality for the whole universe of users. VAS working over Signalling System N° 7, most known as C7 or SS7 [12-13] for Circuit-Switched Core Networks of 2<sup>nd</sup> and 3<sup>rd</sup> mobile communications generations like GSM [14], GPRS/EDGE [15-16], UMTS [16-19], etc., will coexist at least for a decade or two along with LTE/LTE-Advanced worldwide deployments and even the already ongoing definition of 5<sup>th</sup> generation of mobile communications or «5G» [20,104] embracing the «The Internet of Things» concept also known as «IoT». In conclusion, connectivity and VAS based on based on Circuit-Switched networks and SS7/SIGTRAN protocol stack [12-13, 21] encompassing application layer protocols specifically concerned with the establishment, release and control of calls, messaging, and network management like MAP [22], CAP [23-24], ISUP [25], BICC [26], etc., will concur with those built only over IP like GTP [27-28], SIP [29-30], Diameter [31-32], etc., inherent to Packet-Switched networks like the «Evolved Packet System» or EPS [8-9] of LTE/LTE-Advanced, and the «IP Multimedia Subsystem» or IMS [33-35].

## 1.2 Definition of the problem

Given the scenario described until this point, the need for providing solutions to escort NGN deployments with transient continuity of legacy Circuit-Switched Core Networks is advised.

As described by IT and Telecom business analyst expert Alan Quayle [120], an opening rest among the following topics:

- Legacy telecom infrastructure will remain a key asset for quite a long time.
- Moving from traditional vendors to FOSS (Free and Open Source Software) for lower cost and more flexible core network components.
- Shift to IP communications is accelerating.

- Real Time Communications is still out of reach for most Web and Mobile App developers.

## 1.3 Motivational Scenarios

Concomitantly with LTE worldwide deployments including the ones taking place in Colombian territory, there are projects of national interest in course, as the Colombian Ministry of Information Technologies and Telecommunications (MinTIC) «National Network of Emergency Telecommunications» or «RNTE» as for its Spanish acronym [36-37], as well as the «Promotion of mobile financial services (MFS) and follow-up action for content and applications provision» specified in the yellow document of the Commission for the Regulations of Communications by October 2013 [38]. These two endeavours perfectly fit as motivation scenario for developing the Master of Science work purpose of this document, as they expose voids according to ongoing technical specifications and corresponding deployments in today's evolving networks, as it will be comprehensively exposed.

Taking into consideration the MFS proposal from the CRC with regard to compulsory universal provision of mobile banking services via «Unstructured Supplementary Service Data», better known as USSD [39-42], it's unmistakably manifested the technical provisioning of the service through Circuit-Switched networks through MAP from SS7 protocol stack, meanwhile it's not the case for IP based radio access and core networks like the IMS and LTE/LTE-Advanced, where USSD shifts towards a SIP based trade-off as specified by 3GPP/LTE in [42], also known as USSI.

Regarding the RNTE, breaches emerge from the proposal, either for the efficient upload/download of alarms and operational information, as well as Location Services (LCS) in Next Generation Networks like LTE and the IMS under which, according to 3GPP/LTE technical specifications [43-45], are carried out in the control plane by means of Diameter extensions developed for geographical coordinates retrieval from a specific roaming mobile device.

It's also noticeable a remarkable absence of these solutions either regarding USSI or LCS among recently deployed LTE networks.

Besides Colombian national projects like the ones mentioned un previous paragraphs, further international ones like United States of America's National Emergency National Association (NENA) «NG911» project [105] or Peruvian «Stalker Law» [106] fit in the same direction as motivational scenario for this research.

## 1.4 Scope

The main concern of this study focuses in providing mechanisms for Value-Added Services continuity either over all-IP NGN's or Circuit-Switched legacy networks. Likewise, as already stated, the general objective of this MSc thesis is enabling Value-Added Services deployment within heterogeneous networks environments, by developing transparent messaging and positioning mechanisms according to international standardization organizations, with focus on 3GPP/LTE technical specifications.

So as to narrowing this wide research field into a feasible MSc academic project, and at the same time keeping congruence with the mentioned motivational scenarios, the following research quest emerges: How to provide Location Based Services (LBS) triggered by asynchronous messaging events according to 3GPP/LTE specifications so as to making them work universally and transparently regardless of user equipment and radio access network?

Select an open source workspace with capabilities for the construction of solutions for heterogeneous telecommunication networks comes as first step, followed by the development of an Application Programmable Interface (API) and enhancement/addition of network resources adapters/enablers for seamless messaging and location services either for legacy or next generation networks. Finally, using evaluation methods according to DESMET [100] methodology will endorse the scope of this work.



## 1.5 Contributions and results

As a result of this work, Open Source developer's community, either from an enterprise or academic environment, are now provided with the means for adding value to their Web services or IoT applications by providing immediate or event triggered location information, regardless of the technology involved, either for the access network the target device is located at, or their coding skills/programmable languages used. Moreover, this location data can be triggered by several means, either from plain HTTP requests, or messaging services like SMS or USSD and even voice across heterogeneous networks, either Circuit or Packet-Switched.

As it will be exposed further, this work also paves the way for future related R&D projects, as some peripheral tasks must be carried out depending on the available network infrastructure.

Finally, following a SOA approach and 3GPP/LTE specification's guidelines, where tasks are stated as «what» should be implemented rather than «how», this project introduces a unique way of achieving its objectives, scrutinized by highly qualified professionals around the area.

## 1.6 Monograph structure

This section describes how the current document is structured.

Chapter 1 covers the overall context, definition of the problem, motivational scenarios, scope of work, contributions and results.

Chapter 2 is about the state of the art involving the matters of this work. A conceptual basis is approached in the first place, where a chronological transition of value-added services and IT paradigms either for Circuit-Switched or Packet Switched Core Networks is briefly described. Academic and industry's related works survey carried out during this work is then portrayed, followed by a brief description of

main concerns of this work, i.e. location and messaging services in cellular networks, regardless of the type of access or network generation.

Chapter 3 describes the Open Source framework chosen for this work. Derived from the Mobicents project, and besides being the most successful Open Source Telecommunications project in terms of activity, contributors, commits as can be deduced from [128], RestComm appears as the perfect choice as it suits all needs for the problem addressed.

Chapter 4 covers the core topic of this work, the RestComm Geolocation API. Designed and developed strictly to satisfy the motivational scenarios presented at this work (among others), RestComm Geolocation API provides Web or Mobile developers a «SOA» approach interface for performing location services in all kinds of wireless networks (including cellular, regardless of the type of access), without the need of understanding underlying network technology protocols.

Chapter 5 illustrates about RestComm Gateway Mobile Location Centre and needed work to achieve this work purposes. In other words, the development done for allowing it retrieval of mobile equipment location information regardless of the Radio Access and Core Network it is attached to. It also provides a brief about jDiameter and the implementation carried out of SL<sub>g</sub> and SL<sub>h</sub> interfaces for LTE Location Services as specified in 3GPP/LTE specifications [44-45]. Beyond this work, not only RestComm jSS7 but also RestComm jDiameter comprise the low-level protocol stacks of RestComm GMLC core network element.

Chapter 6 describes the evaluation of this work, which given its characteristics and massive telecommunication's assets needs, comprises the description of the DESMET methodologies used.

Chapter 7 provides the conclusions of this work, including obtained results and future work.

## Chapter 2

### 2 State of the Art

#### 2.1 Conceptual basis

Telecommunications has turned out to be one of the most profitable business in the world since the invention of modern telephony and particularly, since the introduction of wireless mobile communication. During the early 1970's Bell Labs and NTT (Nippon Telegraph and Telephone) separately initiate research for first generation of mobile radio communications or cellular telephony. Between 1981 and 1983, the first commercial cellular networks are launched in Europe, the United States of America and Japan, namely:

- NMT-450 (Nordic Mobile Telephone System). Transmitted in Frequency Modulation (FM) at 450 MHz in the media plane (voice) and FFSK (Fast Frequency Shift Keying) modulation in the control plane (signaling). It's the first mobile communication system that introduced concepts like roaming and handover and operated in Sweden, Norway, Finland and Denmark. Later, NMT 900 was introduced in the 900 MHz radio electric spectrum band across the European Union.
- AMPS (Advanced Mobile Phone System). Product of Bell Labs and originally specified by ANSI as EIA/TIA/IS-3 (1982), then EIA/TIA-553. Operated in FM at 850 MHz in the media plane (for 30KHz bandwidth) and used FSK (Frequency Shift Keying) in the control plane (signaling). Besides the USA, it also operated in Australia, Southeast Asia and Africa in its first stages.
- TACS (Total Access Communication System). Developed by Vodafone and Cellnet within General Electric premises (later, Motorola) in Lynchburg, Virginia,

USA. It constituted a variant of AMPS, later introduced in the United Kingdom as ETACS by 1985. It operated in FM at 900 MHz for a 25 KHz bandwidth in the media plane (voice), and also FSK at 6.4 KHz in the control plane (signaling).

- JTACS/NTACS (Japan/Nippon Total Access Communication System). Japanese version of TACS.

It becomes of significant importance at this point to clarify the difference between the media and control plane, as it comprises a vital concept throughout this work, especially when referring to signaling. The media plane is the channel used for transmitting user's payload (voice in the early stages of cellular communication, audio/video and other data in further stages). Meanwhile, the control plane is the one dedicated for signaling, which is best defined in ITU-T Q.9 [123]: «*The exchange of information (other than by speech) specifically concerned with the establishment, release and other control of calls, and network management, in automatic telecommunications operation*». The purpose of signaling can be then demarcated as the mechanism for control information among telecommunication system entities by which several capabilities become available, namely: supervision (condition detection or state change), traffic control, addressing for service establishment and/or release, access to data bases, OA&M (Operation, Administration and Maintenance). Signaling System N°7 or Common Channel Signaling System No. 7 (SS7 o C7) embraces the global standard for signaling in Circuit-Switched Telecommunications Core Networks defined under ITU-T, with variants such as the ones from European Telecommunications Standards Institute (ETSI), the American National Standards Institute (ANSI) y Bell Communications Research (Telcordia Technologies). Please refer to Annex A for a further detail summary on SS7.

As the huge leap as first generation of cellular communication represented, its limitations soon became clear along with its success. Some of those shortcomings are listed next:

- Incompatible networks: «roaming» between networks was unattainable.
- Security issues: networks were susceptible to Electronic Serial Number (ESN) and Mobile Identification Number (MIN) cloning due to lack of effective security mechanisms at the analogue access.
- Low capacity or poor bandwidth.
- Radiofrequency spectrum inefficiency.

It was during those years of incompatible technologies proliferation when the European Conference of Postal and Telecommunications Administrations (then CEPT for, now Electronic Communications Committee [124]), creates a new standardization forum named «Groupe Spéciale Mobile», to elaborate a unique mobile digital communication system for Europe in the 900 MHz band. This work derived in what it was later known as GSM (Global System for Mobile). GSM development starts by 1988 and is commercially launched in 1991, becoming the de facto European standard of mobile digital telephony, specified by the European Telecommunications Standards Institute (ETSI). Meanwhile, in the United States of America ANSI IS-54 technology is launched by 1988, also known as Digital AMPS. By 1993, the American second generation of digital mobile communications is deployed under the IS-95. Almost simultaneously, DCS 1800 (Digital Communication System 1800), is launched in Europe (which is no other thing than GSM transmitting in the 1800 MHz band). By then, Japan had evolved from NTT, JTACS/NTACS analogue systems to its own digital second generation one known as JDC (Japan Digital Communications). Table 2.1 summarizes the main technical aspects around the aforementioned second generation of mobile digital communication systems.

By late 1980's and early 1990's new concepts were introduced like the Integrated Digital Services Network (ISDN), which defined signalling principles over which almost all these digital core networks are based on. Aiding this digital communications progress, Intelligent Networks (IN) emerges as a supplement to lift the control over Circuit-Switched calls to a higher-layer platform. Later, IN concept falls into mobile networks under the project known as CAMEL (Customised Applications for Mobile Enhanced Logic) [22-24]. CAMEL was specifically developed for GSM (and subsequently for GPRS/EDGE and the UMTS) and defines several types of typical IN operations for mobility, namely: control of Circuit-Switched Call/GPRS/SMS, Online charging, USSD control, Supplementary Services (SS) invocation notification, Mobility Management, control/interrogation/modification of CAMEL Subscription Information (CSI), Location/Status Any Time Interrogation (ATI), Mobile Number Portability (MNP), etc. Please refer to Annex A for a further detail summary of CAMEL main concepts.

Second generation mobile communications were incompatible among several technological topics such as radio access methods, modulation schemes, communication protocols, etc., as briefly depicted in Table 2.1 Hence, as mobile communications became a worldwide basic need, these issues, and especially the impossibility to provide roaming outside the Home Public Land Mobile Network (H-PLMN), comprised a huge global problem for each player among this already huge industry. GSM turned out being the most successful and widespread 2G digital mobile communication system, among many reasons, but mainly for the introduction of the SIM (Subscriber Identity Module).

Characteristics	2G Digital Telephony System			
	GSM	IS-54	JDC	IS-95
Region	Europe/Asia	U.S.A.	Japan	U.S.A./Asia
Access Method	TDMA/FDD	TDMA/FDD	TDMA/FDD	CDMA/FDD
Modulation Scheme	GMSK	$\pi/4$ -DQPSK	$\pi/4$ -DQPSK	SQPSK/QPSK
Frequency Banc (MHz)	935-960 890-915	869-894 / 824-849 1477-1489 / 1429- 1441 1501-1513 / 1453- 1465	810-826 840-856	869-894 824-849
Carrier space (KHz)	200	30	25	1250
Channels/carrier	8	3	3	Variable
Channel bit rate (Kbps)	270.833	48.6	42.0	1228.8
Voice codification	13 Kbps (A law)	8 Kbps ( $\mu$ law)	8 Kbps ( $\mu$ law)	1-8 Kbps ( $\mu$ law)
Frame duration (ms)	4.615	40	20	20

Table 2.1. Technical aspects of main 2G mobile communication systems.

Regardless of its success, MNOs with already deployed GSM networks, soon were pushed to the addition and improvement of services in a global market, technologically increasingly demanding and eager for reliable information and agile access.

As technology progressed, so did the available services and vice versa. In other words, a constant virtuous circle emerges between customer needs and services. Being voice the first value-added service in telecommunications, other ones such as short text messaging services (SMS, USSD), multimedia messaging service (MMS), high definition audio, video, etc., became a natural necessity mobile communications. The arrival of Internet accelerated further these demands, not only along the market of personal computers, but also mobile devices. This became part of the convergence of telecommunications concept. While the Circuit-Switched Core Network (CS CN) is capable of transporting these data, it is becoming less and less viable and therefore, a Packet-Switched Core Network (PS CN) surges as the answer to this problem. GPRS (General Packet Radio Services) implementation among GSM networks narrowed the breach between mobility and the Internet becoming the first PS CN among cellular networks. From the architecture point of view, GPRS introduces two main nodes comprising the first Packet-Switched Core Network (PS CN), through which a connection may become established between a mobile station and Packet Data Network (PDN), namely: SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node). Even though GPRS brought connectivity to the Internet to the mobile subscriber, it did not become the optimal or near final solution. Consequently, EDGE (Enhanced Data for GSM Evolution) is deployed with the objective of improving data bandwidth and then, mobile data service quality. It soon turned out not being enough too. Please refer to Annex B for a further detail summary of GSM and GPRS/EDGE network topology and main concepts behind their architecture design.

Albeit GSM becoming the most successful mobile communication system, other second generation digital systems were already there and just replacing them was not an option in the short term. In the dawning of third generation of digital communication systems, it became evident that something needed to be done towards a common standard. Hence, under the aegis of ITU, IMT-2000 (International Mobile Telecommunications-2000) is created as the global standard for third generation mobile communications. IMT-2000 is then the collaboration outcome of different standards groups and aims at providing telecommunications services access using radio links, including terrestrial and satellite networks. IMT-2000 ensue 3GPP (Third Generation Partnership Project) and 3GPP2 (Third Generation Partnership Project 2) standards. Their technical specifications arise by 1998 via the collaboration

of all the main players in the telecommunications industry, including ETSI (European Telecommunications Standards Institute), Japan's ARIB (Association of Radio Industries and Business), CCSA (China Communications Standards Association), United States of America T1 Committee, South Korea's TTA (Telecommunications Technology Association), Japan's TTC (Telecommunications Technology Committee).

Meanwhile 3GPP comprises a set of technical specifications and reports (TS - Technical Specifications; TR - Technical Reports) for the third-generation mobile telephony system known as UMTS (Universal Mobile Telecommunications System) based on the dominant second generation digital system worldwide to date, i.e. GSM, 3GPP2 surges for the evolution of North American and Asian standards based on ANSI/TIA/EIA-41 and cdma2000 towards a third-generation system. 3GPP2 organization partners are the same of those of 3GPP with the addition of TIA (Telecommunications Industry Association). Besides, other 3GPP/3GPP2 partners result from the need of different markets convergence. This partners include, among other, the UMTS Forum, 3G Americas, GSMA, OMA, TISPAN, TD-SCDMA Forum, IPv6, etc.

One key element that also surges as a key piece of architecture from 3GPP/3GPP2 specifications is the IP Multimedia Subsystem (IMS), introduced by release 6. The IMS main objective is providing ubiquitous cellular access to all those services already available in the Internet. Please refer to Annex C for a further detail summary of 3GPP UMTS and IMS network topology and main concepts behind their architecture design.

The original «Release 99» specifications of UMTS introducing were have been extended with High-Speed Downlink/Uplink Packet Access (HSDPA and HSUPA or collectively High-Speed Packet Access or HSPA). Beyond 3GPP Release 7, HSPA improved to HSPA+ as for higher-order modulation and the introduction in cellular communications of MIMO (Multiple Input Multiple Output).

Constant evolution of technologies and services need towards telecommunication networks and services convergence, moved forward mobile communications (and cellular networks in particular) under the model known as Long



Term Evolution (LTE), specified beyond the 8<sup>th</sup> release of 3GPP specifications. LTE comprises an entire Packet-Switched «all-IP» architecture network, in order to providing IP connectivity to either the end user and its UE (User Equipment) and a PDN (Packet Data Network), without service interruption along user's applications due to mobility, thus making it possible to access either «Voice over IP» (VoIP) (through popular applications like Skype, WhatsApp, Viber, etc.) or data services such as file downloading, HTTP web browsing, etc.

Meanwhile the LTE term is widespread used for the evolution of the UMTS radio access network or E-UTRAN (Evolved UMTS Terrestrial Radio Access Network), such advancement is further escorted by aspects non-related with the radio-electric coverage enhancements, like the ones under the «System Architecture Evolution» (SAE) concept, which involves the «Evolved Packet Core» (EPC) network. Together, LTE and SAE comprise the «Evolved Packet System». EPS embraces the «EPS bearer» concept to route IP traffic from a PDN to the UE. An EPS bearer constitutes an IP packet flow with a defined «Quality of Service» (QoS) between the UE and the PDN. Then, E-UTRAN and EPC jointly establish and release EPS bearers while requested by the applications.

The E-UTRAN is responsible of the entire functions related with transmitting over the radio-electric spectrum assigned to LTE operators, including radio resource allocation, IP packet header compression, radio data encryption, EPC connectivity, high availability and load balancing. LTE develops the concept of a Self-Optimizing Network (SON). SON functions are key differentiators of LTE against previous UMTS UTRAN/HSPA or GPRS/EDGE GERAN, allowing the MNO to automate significant aspects of network configuration processes, thus reducing the need for centralized planning and human intervention. Meanwhile, the EPC defines a whole new set of network entities which simplify network infrastructure/architecture and therefore improve performance while reducing bit traffic cost.

While 3GPP/LTE progress in EPS is obviously in constant mode towards a fifth generation, it does not mean that further development of the other 3GPP radio access or core network technologies ceased (e.g. HSPA+ and UMTS). These backward-compatible enhancements enable MNOs that heavily invested in UMTS' WCDMA (Wideband Code Division Multiple Access) to generate additional revenue from next

generation value-added services while still delivering to their existing subscribers using legacy terminals. Moreover, EPS provides interfaces and network entities which anchors the user plane across E-UTRAN or previous 3GPP radio access networks (UTRAN, GERAN) -as well as other non 3GPP access networks like cdma2000 or WiMAX-.

Standardization in 3GPP2 has continued a parallel evolution towards data-oriented systems (EVDO). However, LTE will provide tight interworking with systems developed by 3GPP2, thus allowing operators which previously followed the 3GPP2 track (for IS-95 and cdma2000 retro compatibility) a smooth migration to LTE and beyond systems specified by 3GPP only.

LTE-Advanced objectives were portrayed to be accomplished by 3GPP/LTE release 10 specifications (2011) and beyond so as to accomplishing the 4<sup>th</sup> generation goals specified by IMT-Advanced (4G). Other standardization groups such as the IEEE and WiMAX Forum have been developing wireless access standards according to IMT-Advanced specifications. Also, full Packet-Switched oriented, IEEE 802.16e is the first product of such efforts, also known as “Mobile WiMAX”. One important initial difference of WiMAX standards was that it was not designed with the same emphasis on mobility and compatibility with MNO’s core networks as 3GPP standards, which core network evolutions to escort radio access network enhancements. Therefore, the «WiMAX family» developed IEEE 802.16m for interoperability with IMT-Advanced systems, i.e. LTE-Advanced and WiMAX 2. Both technologies make extensive use of OFDMA (Orthogonal Frequency Division Multiple Access), MIMO, turbo coding, intelligent scheduling, link adaptation to channel quality and cooperative access networks (relaying). Although it is important to introduce them, no further reference to non 3GPP/LTE standardization groups technologies will be subject of this document hereinafter. Please refer to Annex D for a further detail summary of 3GPP LTE/LTE-Advanced network topology and main concepts behind its architecture design.

Figure 2.1 portrays the evolution of main wireless digital technologies covered until this point.

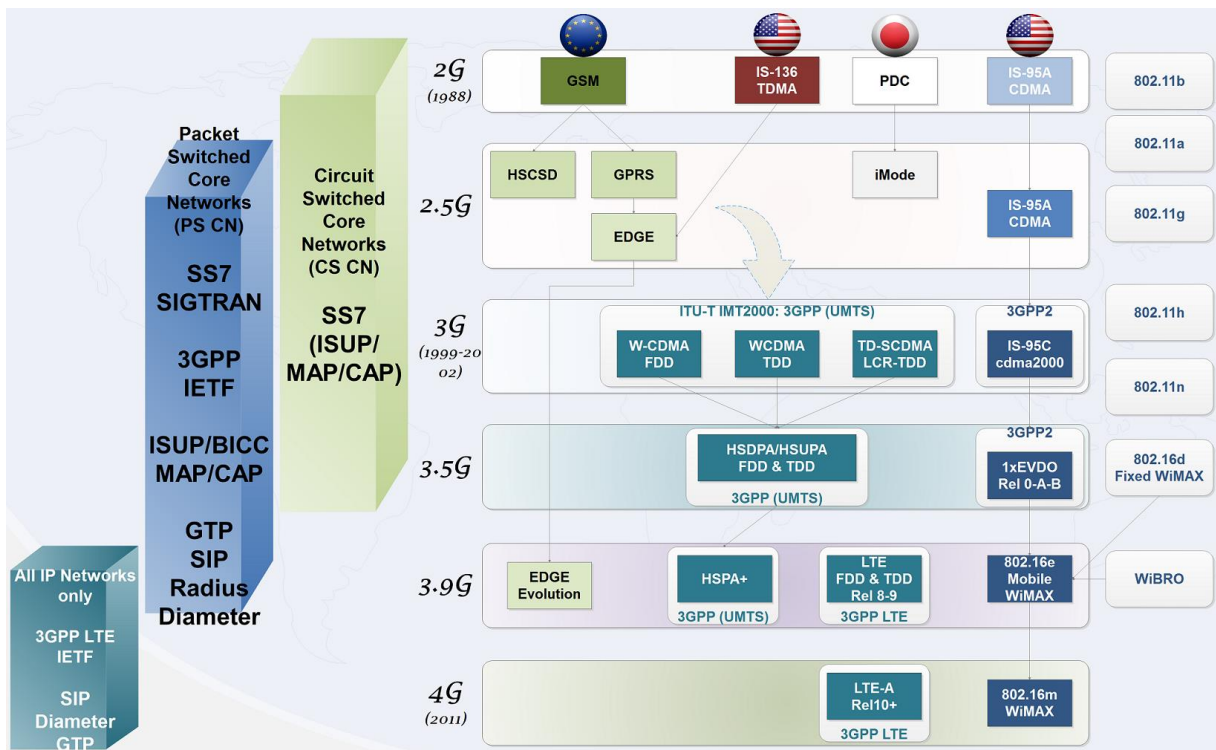


Figure 2.1. Worldwide wireless technologies and standards evolution.

Figure 2.1 provides a graphic survey of what’s been detailed chapter 1 and particularly in section 1.1 of this document in terms of VAS being shifted from being conveyed in Circuit-Switched Core Networks over SS7 stack protocols to those ones over IP like SIP, Diameter, etc., in Packet-Switched Core Networks. Please refer to Annex E and F for a further detail summary of SIP and Diameter control plane protocols for VoIP and NGN.

Next Generation Networks or «NGN» [115-116] paradigm stems from the limitations imposed by both legacy fixed and mobile «Intelligent Networks» or «Customised Applications for Mobile Enhanced Logic» (IN/CAMEL [24]) regarding to third parties’ collaboration in service creation, network infrastructure loose coupling and lesser time-to-market. NGN afford sharing resources and infrastructure capabilities to CSPs, simplify internetworking, ease and unify services management, operation and maintenance, thus enabling a fast and cost-effective creation of new and customized ubiquitous wideband services. Final users become then enabled to enjoy Telco mobile services with the same flexibility, scope and variety they’ve been

already enjoying through the Web (Internet). Hence, the IMS can be placed under the NGN classification.

Service-Oriented Architecture or «SOA» model adoption within a telecommunication organization is closely related to NGN (Next Generation Networks). NGN provide MNOs the ability to share resources and infrastructure, enable network interoperability, simplify and merge management, operation and maintenance of the offer, thus allowing swift and cost-effective creation of new and custom-made ubiquitous wideband services. These new facilities allow third parties to take advantage of telecommunications capabilities within their own development environments. Likewise, final customers may find new services previously banned due to legacy networks' transmission latency, weak performance, etc.

MNOs without SOA adoption follow an architectural model of closed monolithic applications, where business roles depend on these hermetic silos. This tightly coupled model is highly inefficient and brittle compared to SOA, where a reusable services oriented system is promoted by applications and business rules alignment. SOA offers a bunch of principles for the construction of complex, loosely coupled, autonomous and granular applications. Equally, it defines patterns for the composition of self-described services for accomplishing interoperability between software platforms, as well as dynamic interaction among business processes. In this frame of mind and just to remark the importance of what's being stated thus far, Telefonica's CIO recently admitted a five years' lag of adopting its business-led application transformation on the TM Forum IT standard basis and SOA [117] during his speech at the 2015 Amdocs Latin America Business Summit.

Alongside, the hype around the success and promises of Cloud Computing, SDN (Software Defined Networking) and NFV (Network Function Virtualization), sponsored among others, by large enterprises such as Amazon, Google, Yahoo, Salesforce and Microsoft, as well as the offers of significant organizations such as IBM, Oracle, VMWare, Cisco, Ericsson, Intel, HP, Metaswitch Networks and many open source projects like Project Clearwater, must be tackled as it is in fact a significant Telco concern nowadays.

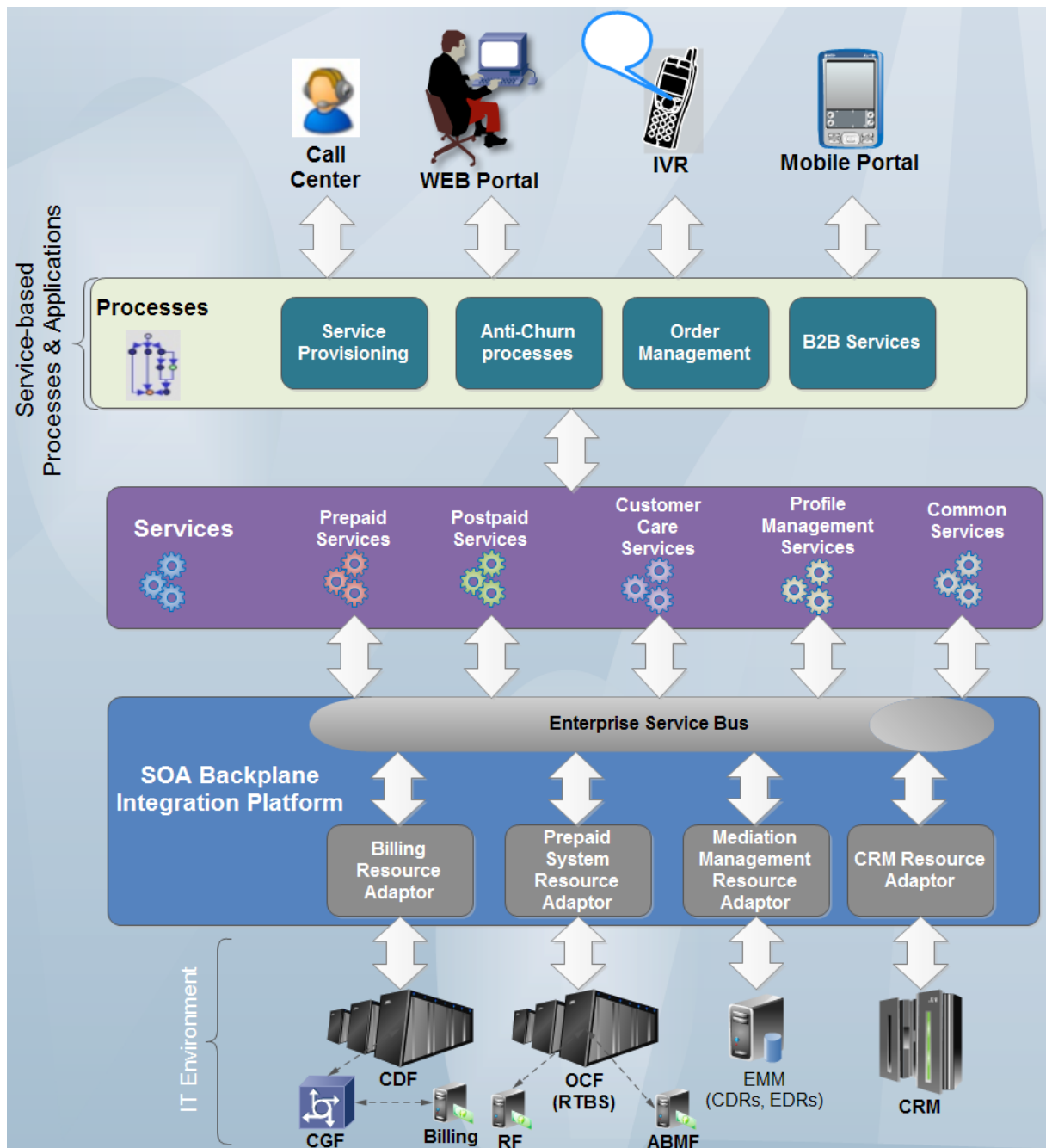


Figure 2.2. Telco service flow with integrated SOA backplane.

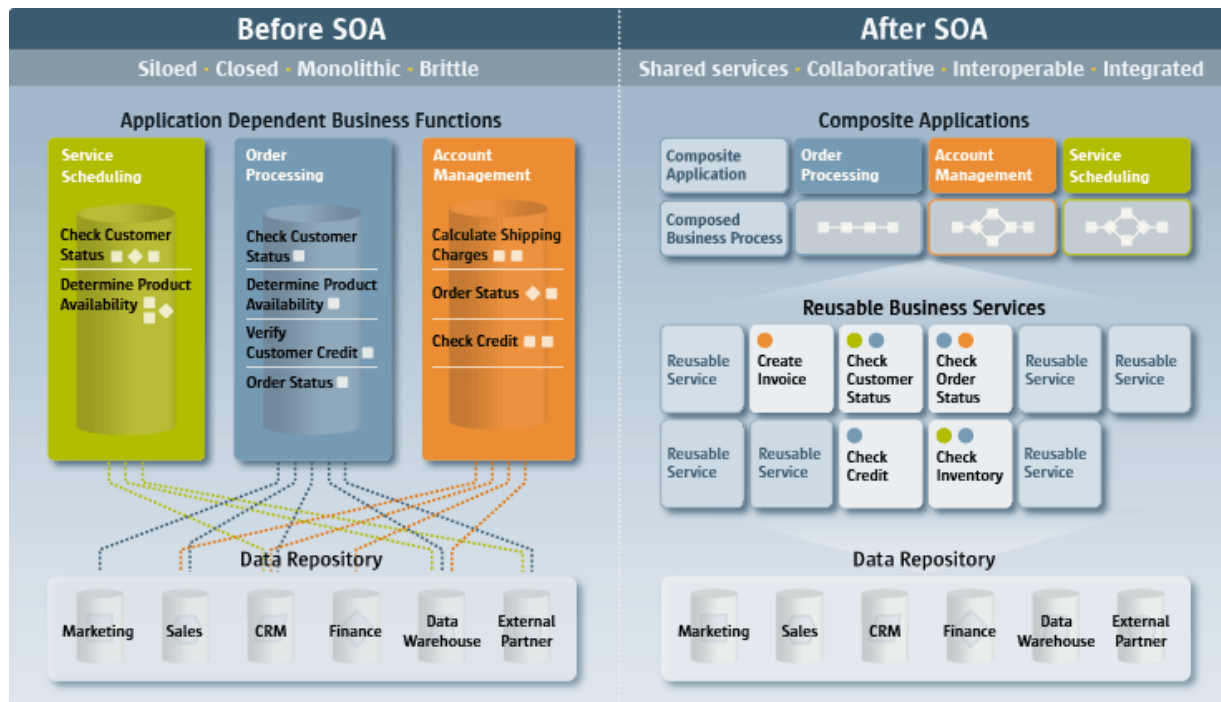


Figure 2.3. Telco business roles example before and after SOA. (Source: Journal of Software and Systems Development [118]).

Telecommunication networks management models also needed a transformation, adjusting and embracing this evolution imposed by the NGN deployment under SOA paradigms. Standardization organizations such as TM Forum and ITU-T converge in NGN management under the acronym NGOSS (New Generation Operations Systems and Software). Between 1995 and 1996, TM Forum matures the TOM (Telecom Operations Map) concept, which itself evolves into eTOM [127] (enhanced TOM), released under ITU-T Recommendation M.3050 series, replacing the TMN (Telecommunications Management Network) way under ITU-T Recommendation M.3010. The main difference between eTOM and TMN relies on management approach; while TMN was built upon network architecture and infrastructure management requirements (bottom-up), eTOM basement relies on the necessity of global support of the entire processes inward the service provider organization (top-down). eTOM focus resides on business processes used by service providers, relationships among procedures, interfaces identification and usage from multiple processes of information about clients, services, resources, providers and

associates. eTOM relates with other standards and frameworks which above all include SOA and ITIL® [8].

So, a brief on the evolution of mobile network infrastructures, networks, protocols, management, etc., towards a global convergence of multimedia services has been covered until this point, deepening on the overall context and definition of the problem as stated in sections 1.1 and 1.2 of this document. Hereinafter, this chapter will focus in the state of the art concerning motivational scenario and scope of this work, as pointed out in sections 1.3 and 1.4. Hence, related R&D works and an introduction to VAS including Location Based Services and messaging will be covered next.

## 2.2 Related Works

Regarding the current state of knowledge concerning the stated problem, this section will begin cataloguing the themes around which has carried out a search of publications related to the problem statement, namely: heterogeneous networks, interoperability among legacy and Next Generation Networks, Location Based Services (LCS/LBS) and messaging services such as USSD/USSI and SMS.

The search engines used were those more often used by the scientific community, namely, IEEE Xplore, ScienceDirect, Springer and ACM (directly or indirectly through their Web portals or via Google or Microsoft engines used by «Harzing's Publish or Perish» tool). Other sources of information further from the referred here, emerged from professional social networking through LinkedIn or from previously studied bibliography. Lastly, related publications within the themes of the problem proclamation, demonstrate an academic interest in the following issues:

- ❖ Stipulate convergence scenarios and conditions between NGN and legacy networks.
- ❖ Agree on the preferred framework for a Telecommunications «*Service Creation/Execution Environment*» (SCE/SEE), consistent with the «Service

Oriented Architecture» paradigm [46-47], accordingly with resource adaptors for the abstraction of underlying network capabilities.

In summary, from the publications detailed in this paragraph, the main contributions are given below:

- ✓ Confirmation of the use of USSD as the favourite channel for numerous VAS implementations as a result of efficiency in the use of network resources, operating costs and independence of user equipment for universal access;
- ✓ Ratify the methods of locating mobile user equipment in legacy and Next Generation Networks, and particularly, over LTE / LTE-Advanced, namely:
  - MAP operations usage for querying legacy networks nodes (SMLC/SMSC/IF-SM-GW/HLR/MSC/VLR; SGSN);
  - Usage of Diameter in the control plane for specific mobile handset geographical information retrieval (in terms of universal geographic coordinates and Global Cell Identity) among LTE's Evolved Packet System or EPS, according to 3GPP/LTE technical specifications [43-45], which define procedures to carry out between a GMLC (*Gateway Mobile Location Centre*) and other entities of LTE/LTE-Advanced Evolved Packet Core (EPC) like the MME (*Mobility Management Entity*), HSS (*Home Subscriber Server*), E-SMLC (*Evolved-Serving Mobile Location Centre*), eNodeB and UE (*User Equipment*). It is important to notice the guidelines for LCS within the user and control planes like OMA's SUPL [62, 108] and MLP [107] protocols for mobile device location.
- ✓ An overwhelming confluence towards JAIN SLEE [68] architecture and particularly, the Open Source platform Mobicents [69], is observed (nowadays rebranded as RestComm [109] Open Source projects by TeleStax [110] -start-up owned by the creators of Mobicents-).

In addition, and with the intention of finding affinities with the announced problem, publications like [49-54], address the usage of USSD and SMS for VAS, meanwhile other publications like [54-67, 113, 128] report available methods for LBS/LCS in mobile networks, either for legacy or Next Generation Networks. As it addresses either subjects, a special consideration is attended to PhD candidates from



Charles and Czech Technical University in Prague work concerning location tracking of mobile devices [54], framed under an «RDC» [93] project, tightly in collaboration with Vodafone's operation in the Czech Republic.

Deepening in reference to the state of the art for the problem raised according to the mentioned search criteria, doubts are cleared and opportunities advised for research contributions, disclosing the most significant gaps in following paragraphs.

No research works are found regarding location information retrieval of mobile equipment for LTE/LTE-Advanced networks applying Diameter extensions according to methods and topology given in 3GPP TS 29.171/172/173 [43-45]. Adding to the previously mentioned divergent approach concerning USSD and SMS utilization related to the work in [54], this labour obtains the least precise positioning information from an inquiry to the HLR by a MAP ATI procedure (mobile network code, mobile country code, location area code, global cell identity and age of location information). This procedure, unique to SS7 based Circuit-Switched core networks, holds an error range much superior to the minimum acceptable according to regulations like the ones pointed out in [57]. Even though it is important to settle that our approach also pursues universal access, it privileges precision in order to accomplish the regulatory requisites or basic demands such as the ones of the RNTE. Given the motivational scenario of our work, the eventual costs in resources for the retrieval of mobile location information, took into consideration in [54] as a mandatory fulfilment influence criterion for the selection of a tracking method, they do not outweigh the precision goals pursued by us for this post graduate project. Besides, our approach embraces a longer term methodology, as Circuit-Switched core networks and methods based on SS7 protocol stack will become globally obsolete in a period no longer than two decades. Additionally, related publications from research Centres involving SIP presence methods for triggering location services do exist as in [64-66]. In conclusion, an academic reference framework for contrast of methodologies and products of unquestionable up-to-date value exists, which also has the potential to becoming an international research and development cooperative effort.

Convergence scenarios described between legacy and Next Generation Networks do not involve the last for the latter regarding USSD/USSI and Location Services as they are more oriented to conference services or for SMS as in [70-72]

and [73-74] respectively. It also highlights the lack of deployments of USSI in LTE/LTE-Advanced networks (consistent with the fact that novel specifications do not involve EPC nodes yet), so as to giving continuity to classic legacy network Value-Added Services such as subscriptions, top ups, mobile payments/banking, balance inquiry, polls, etc., transparently and without the need of third parties applications to be deployed, such as the one set up by the «USSDx» platform from Balefyre [75], only up-to-date known USSD over IP end-to-end implementation, not outlined by 3GPP specifications, as it can be determined in its online brochure, involving a proprietary protocol based on HTTP which further requires the installation of the «emDial» application at the user equipment.

In addition to the facts perceived for USSD/USSI commented in the previous paragraph, within Circuit-Switched Core Networks and, specifically, among VAS over SS7 protocol stack, ceaseless publications contrast USSD vs SMS. In contrast, no mention is observed for LTE and the IMS. Given the fact that USSD and SMS over LTE and the IMS are outlined under SIP protocol guidelines, but involving different modes of work, i.e. SIP MESSAGE transaction for SMS versus SIP INVITE transactions for USSD, its evaluation and results comparison between both methods would confer valuable facts for the R&D community involved in VAS development, either for mobile network operators or mobile services developers. For example, the doctorate work described in [54], comprising of a tracking method for mobile location initiated by network initiated SMS, concludes in performance and resources utilization measurements based on parameters such as amount of located devices, tracking interval, signaling resources utilization either concerning core network or radio links and UE battery consumption. Beyond their arguments, our approach differs from using SMS over USSD. Several publications recognize the advantages of USSD over SMS in terms of efficiency of resources usage, swiftness and cost-effectiveness for mobile network operators [49, 52]. Moreover, results unveiled in terms of growing usage of control channels at the radio interface, i.e., the Standalone Dedicated Control Channel (SDCCH) due to SMS submission, warn about increasing blocking probability for traffic channels. In contrast, the results published in [91] reveal almost null blocking probability of traffic channels when the SDCCH is occupied concurrently by USSD sessions. Thus, a discussion setting is given to contrast results of both works. Also, diverging with what was done in [54], our work pursues operations either in the uplink or downlink channels.

Supplementary to the gaps found among scientific publications, commercial platforms or Open Source projects such as Mobicents USSD Gateway [76], nor at the time include USSD over SIP messaging for an IP only environment as specified by 3GPP for the IMS/LTE. Contrariwise, TeleStax' [77] RestComm USSD Gateway [111-112], performs a translation of MAP based USSD messages from legacy networks to SIP transactions according to 3GPP TS 24.390 [42] guidelines for communication with RestComm (or any other capable IMS Application Server). USSI and USSD over LTE approaches are consistent with VoLTE linked to the IMS, signalled via SIP, still under specification, exploration, development, integration and deployment (most of live LTE networks still use Circuit-Switched core networks for voice call establishment and control, under a technique known as CSFB for «Circuit Switch Fall-Back»). It becomes necessary to notice that, analogous to how it is done for pure VoLTE, no specifications exist regarding control procedures for USSD/USSI sessions over Diameter interfaces in LTE/LTE-Advanced like the PCRF (Policy and Charging Rules Function), the HSS and a AAA (Authentication, Authorization and Accounting) server. Furthermore, no user equipment implementations exist for native USSI support.

As described for USSD over SIP or USSI, from the bibliographic quest opportunities emerge concerning LCS in the control plane over Diameter extensions for LTE according to 3GPP/LTE specifications [43-45]. Besides the fact that MNOs are being pushed by regulatory entities to deploy such LCS within their infrastructure, actual deployments are in exploration phase at the moment. Moreover, regarding RestComm Open Source framework, the implementation of such EPC's interfaces, i.e. SL<sub>h</sub> (GMLC-HSS), SL<sub>h</sub> (GMLC-HSS) SLs (E-SMLC – MME), were not in the roadmap as confirmed by Alexandre Mendonça [81] on December of 2013 and corroborated according to the currently implemented Diameter interfaces [99]. In the same manner were consulted other references with identical feedback, such as Travis Russell, author of numerous reference books about telecommunications protocols and architectures such as [12], currently product manager at Oracle and main contributor to the «*The Diameter Group*» at LinkedIn. Given these facts, TeleStax Inc. executive team decided to bring this MSc project as part of its R&D roadmap for its Open Source RestComm platforms, including RestComm itself, RestComm GMLC for cellular network LCS and RestComm iOS and Android SDK for non-cellular (WiFi) location.

By addressing the still existing gaps either in today's network deployments as in the articles referenced in previous paragraphs, taking into account as motivational scenes latent aspects such as CRC's regulation for mandatory use of USSD as a channel for Mobile Financial Services supply, as well as the National Emergency Telecommunications Network (RNTE) for LTE, NENA's NG911 and Peruvian's Stalker Law, it turns out very attractive continuing the research work in this direction and therefore, the development and deployment of certain services enabled for either legacy or Next Generation Networks, namely:

- ✓ Location Based Services (LBS) for either legacy and NGN, including MAP and Diameter extensions for LTE (ELP/LCS-AP) respectively, according to 3GPP/LTE specifications, and SIP procedures for IP location within non-cellular networks, including OMA's MLP.
- ✓ USSD based services for either legacy and NGN, based on MAP or SIP transactions for LTE (USSD or USSDoLTE) respectively.

Accordingly, the implementation of 3GPP/LTE compliant LCS within the control plane via a GMLC built in an open source framework such as RestComm, either for MAP or Diameter extensions procedures (depending on device target radio access), would provide an opportunity for research and development in areas of technological innovation, as well as perfectly fit the purpose of this project.

Likewise, given its ubiquitous and universal access nature, a socially inclusive contribution is pursued in providing VAS services over heterogeneous networks under the premises of 3GPP/LTE for the provision of LBS/LCS, an undoubted contribution to MinTIC's RNTE project. Efforts involving the user plane are discarded given the following: necessity of compliance of user equipment with the World Wide Reference Network; user equipment must constitute an SETs (SUPL Enabled Terminals) in order to be enabled to exchange messages with an SLP; SLP is supported in asynchronous events based on SMS or WAP, relatively inefficient in network resources, not always effective and moreover, not always available as is the specific case of WAP (besides considering the latter, a deprecated technology); it turns to be very complex and costly creating a simulation environment for this kind of solution. Coinciding with the criteria used in [54], we consider more appropriate and long term

effective following 3GPP/LTE and OMA guidelines over the control plane. Besides, these LCS procedures within the control plane for Next Generation Networks such as LTE or legacy networks such as GSM/UMTS rely, respectively, on extensions to Diameter protocol, of broad global development to date, as well as SS7 MAP operations, for which, resource adaptors already exist in RestComm Open Source platforms.

These new capabilities would be possible by developing expansions to RestComm Open Source projects, including RestComm GMLC, jSS7, jDiameter, SIP Servlets and iOS/Android SDKs, by building from scratch a new Application Programmable Interface (API). This API, hereinafter referred as RestComm Geolocation API, becomes then the core element of this work and its main academic/industry contribution, as it gathers all concepts mentioned in related works or specified by standardizations groups under an innovative approach.

Also, and giving continuity to the «TelComp2.0» [83] project, the start of the «Telco 2.0» project, involving the deployment of an NGN/IMS laboratory network, both of them belonging to University of Cauca Telematics' Engineering Group (GIT), constitutes a proper R&D scenario for the thesis outlined here in an academic environment. The extension of this work in a manner that embraces services for legacy Circuit-Switched networks over SS7 protocol stack on one hand (MAP, CAP, etc.) and, at the same time, with the appropriate communication protocols of Next Generation Networks such as the IMS and LTE (SIP, Diameter, etc.) constitutes a big part of the spirit of this work. Moreover, multidisciplinary collaboration possibilities spread wide open with international R&D Centres [93-98], either for the radio-frequency access or the core network. Testing and simulation network environments such as «Open IMS» [83], «Open EPC» [53, 84-85], «Open LTE» [86], «LTE-sim» [87-88], «LTE Simulators» [89], «Open BTS» [90], etc., open the game to the enrichment of Telco 2.0 project. On any licensing agreements with agencies such as the Department of Telematics at the Polytechnic University of Bari, the Institute of Telecommunications of Vienna University of Technology (owners of open source LTE mobility entities simulators under university licensing such as [87-88] and [89] respectively) or «Open EPC» from Fraunhofer FOKUS [94], it is considered highly likely for later motivations to emerge and/or R&D needs of interest for all parties involved.

## 2.3 Location Services in Cellular Networks

Based on numerous publications like [54-67, 113, 128] reporting available methods for LBS/LCS in mobile networks, either for legacy or Next Generation Networks, as well as industry and regulation trends, MNOs are nowadays pushed by regulation entities for high demanding LCS/LBS, for the likes of emergency services provision like NG911 and E112 in America and the European Union respectively, or the RNTE in Colombia, need to have as many technology options as possible to meet these requirements, both in the control and user planes. According to current infrastructure, the following options are available in both planes supporting the aforementioned methods (A-GNSS, OTDOA, UTDOA and AECID):

- ✓ Location information retrieval within the control plane through a Gateway Mobile Location Centre (GMLC) and its counterpart, the Stand-Alone Serving Mobile Location Centre (SAS) for location within the UTRAN (UMTS Terrestrial Radio Access Network) or Enhanced-SMLC (E-SMLC) for location within the E-UTRAN (Enhanced-UTRAN or LTE).
- ✓ Location information retrieval in the control plane through positioning system using OMA's Secure User Plane Location (SUPL) protocol [61-62, 108], also known as SLP (SUPL Location Platform).

Figure 2.1 exhibits interfaces and acronyms of either protocols or network entities for Location Based Services in mobile legacy networks (either CS or PS) such as GSM, GPRS/EDGE or UMTS. SS7 MAP operations are performed for location retrieval either from the HLR via a MAP ATI (Any Time Interrogation) procedure between the GMLC and the HLR, or from the combination of MAP SRIforLCS (Send Routing Information for Location Services), MAP PSL (Provide Subscriber Location) and MAP SLR (Subscriber Location Reports) procedures between the GMLC and the HLR/HSS and SAS (Stand-Alone SMLC).

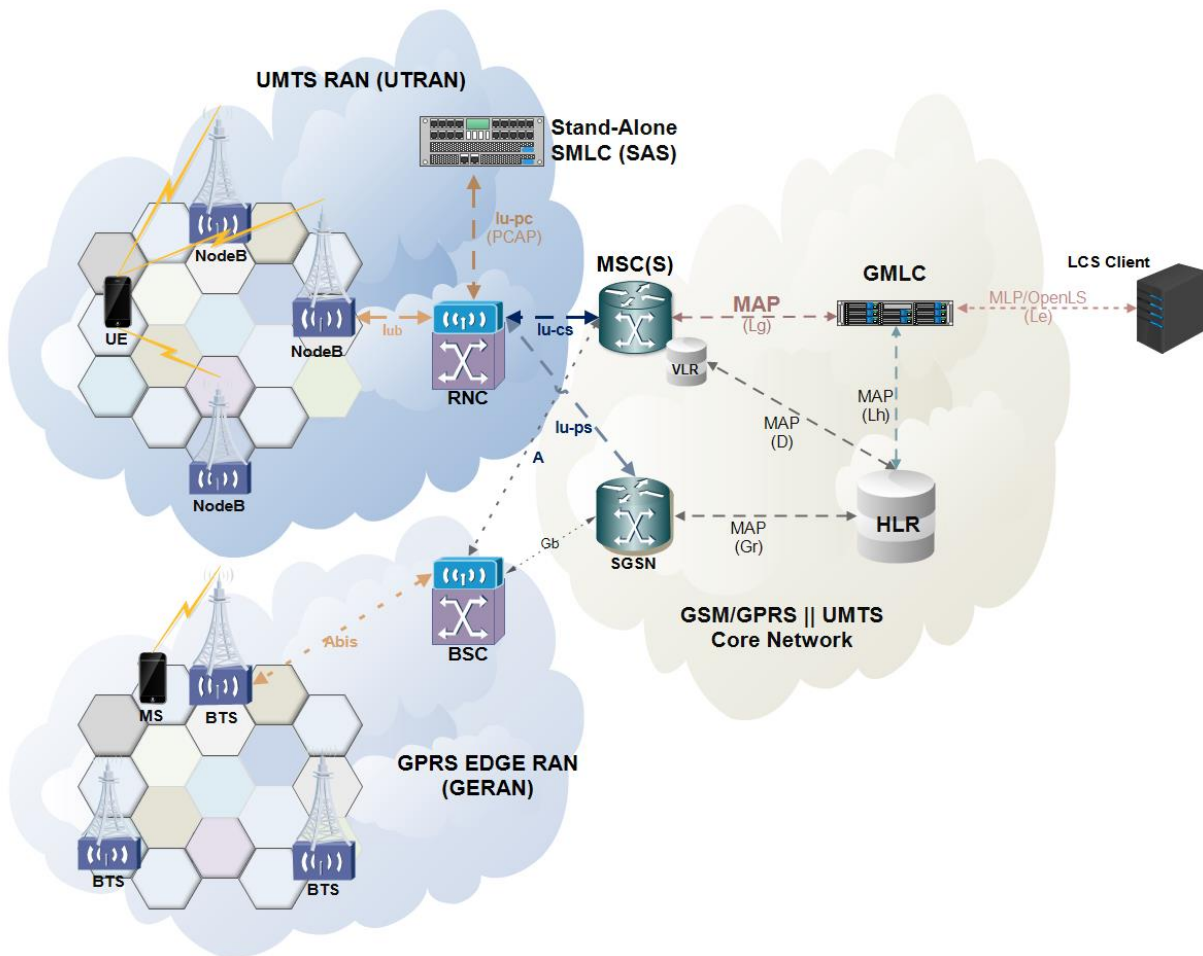


Figure 2.4. Location Services Architecture in GSM, GPRS/EDGE and UMTS according to 3GPP.

Location requests sent to the GMLC through the Le interface are often done using plain XML over HTTP(S), with the request being encoded in OMA MLP (Mobile Location Protocol) [107]. MLP is then an application-level protocol for getting the position of mobile equipment from the RAN through a GMLC.

The simplest location information a GMLC can retrieve is by issuing a MAP ATI (Any Time Interrogation) request to the HLR (Home Location register). MAP ATI is part of CAMEL phase 1 and it does not trigger any location procedure at the RAN. If the GMLC is allowed to proceed with the operation at the HLR, the latter will respond with the Cell Global Identification (CGI) as for the latest MAP UL (Update Location) operation carried out between the HLR and VLR at which the target mobile equipment

is attached too (therefore, an additional parameter known as "Age of Location Information" is also included in the response). As shown in Figure 2.2, CGI is made up of multiple components, namely, MCC (Mobile Country Code), MNC (Mobile Network Code), LAC (Location Area Code) and CI (Cell Identity). The combination of MCC and MNC represents the PLMN at which the cell is located, in other words, the country and Mobile Network Operator it belongs to. LAC represents a geographic location area in which a cluster of Base Transceiver Stations (BTS) are located for radio access, while CI, uniquely identifies the BTS providing service to the target subscriber in that area (more commonly known as cell). From CAMEL phase 4 compliance onward, MAP ATI can also retrieve the IMEI and MS Classmark.

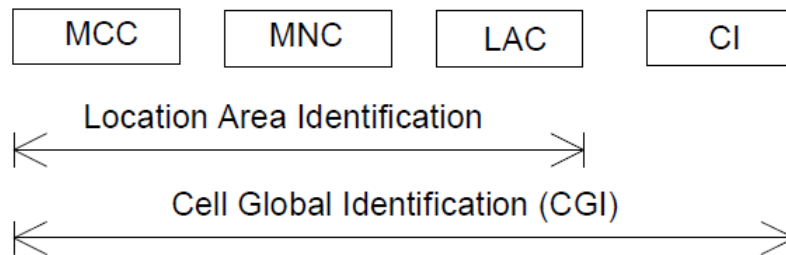


Figure 2.5. Cell Global Identity assembly as for 3GPP TS 23.003.

MAP SRforLCS, PSL and SLR are UMTS procedures which depend on the existence of an SMLC for more precise location information in terms of geographical coordinates. Also, positioning technologies must rely on the RAN as will be described in next paragraphs.

Figure 2.3 portrays interfaces and acronyms of either protocols or network entities considering implementation both in the control and the user plane within an all-IP environment only either at the radio access network (E-UTRAN) or the Evolved Packet Core of LTE/LTE-Advanced, as well as the IMS. Furthermore, a SIP-AS is located, as well as the corresponding interfaces for its functions, either for SIP trunking or Diameter procedures at the IMS and LTE/LTE-Advanced core network. Moreover, in order to accomplish maximum effectiveness and therefore comply with mentioned regulatory demands, a combination of either control and user plane platforms is considered ideal according to [56-60], thus both GMLC and SUPL based interfaces are included.



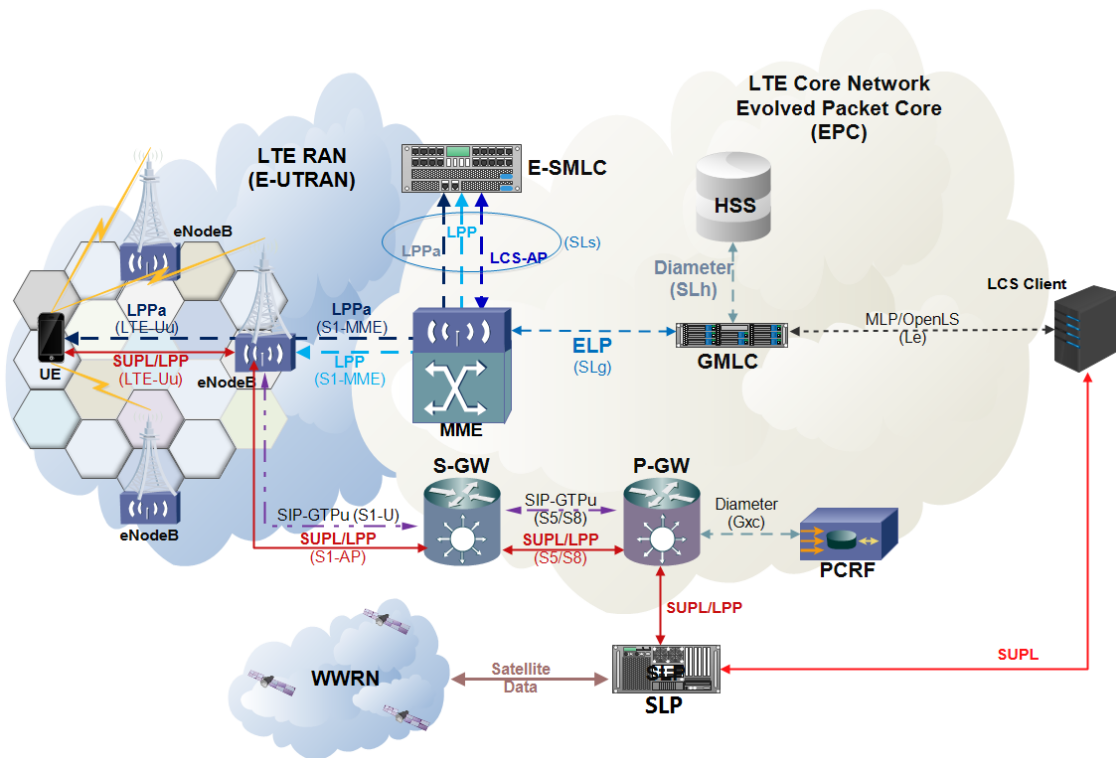


Figure 2.6. Location Services Architecture in LTE according to 3GPP/LTE and OMA.

Several methodologies are used upon Radio Access Networks (RAN) for LCS. Following are briefly described the most used location methods among all generations of mobile RAN, including GSM' Base Station Subsystem (BSS), UMTS Terrestrial RAN (UTRAN) and LTE's Enhanced UTRAN (E-UTRAN):

- **A-GNSS** (*Assisted Global Navigation Satellite System*). It comprises a method based on or assisted by the mobile equipment which performs satellite measurements through GPS, Galileo or GLONASS. It achieves the greatest precision, but not available in legacy mobile equipment and positioning is compromised in urban/indoors environments.
- **TDOA** (*Time Difference Of Arrival*). The TDOA of two signals travelling between the given node and two reference nodes is estimated. This determines the location of the given node on a hyperbola with focal point at the two reference nodes. A third reference node is needed to triangulate the position of the mobile equipment. It is called hyperbolic trilateration because it uses hyperbolas and no spheres or circles. In hyperbolic trilateration, at least

three BTSs are necessary to get a clear position of a mobile equipment. The error margin is between 100 and 300 metres.

- **OTDOA** (*Observed Time Difference Of Arrival*). It consists of a mobile equipment assisted method, based on RSTD (Reference Signal Time Difference) received from several locations across the «Downlink», where location is calculated via trilateration. It achieves good precision (around 100 meters of error margin) and useful in every environment, even those inaccessible to satellites.
- **UTDOA** (*Uplink Time Difference Of Arrival*), whose main differences with UTDOA relies on the fact that it calculates positioning from time difference of arrival of signals in the «Uplink», and that it encompasses a network assisted method.
- **E-OTD** (*Enhanced Observed Time Difference*). Only operational in GSM and GPRS networks. The mobile equipment sends a signal to the surrounding cells BTS, then the nearest one sends back the signal. The time taken between sending and receiving the wave is analysed by an SMLC, which calculates the cell phone position in the network. More accurate in best conditions than xTDOA, but vulnerable to accuracy degradation due to multipath reflections and needs a software update at the mobile equipment.
- **AECID** (*Adaptive Enhanced Cell Identity*). It encompasses a method assisted by the mobile equipment or the network which uses a record of cell identities (CID), several measurements from the base stations, timing advance (TA) and angle of arrival (AoA). Less precise than the latter but available in every environment and useful for handsets not compliant with the GNSS.
- **ECID** (*Enhanced Cell Identity*). Similar to AECID, but angle of arrival (AoA) is not used. Less precise than the latter but much less expensive to set up.

The aforementioned RAN positioning procedures bring up different concerns upon the following subjects, as covered for instance in [113], namely:

- Accuracy (where error margin determines accuracy levels)

- High: error margin lower than 50 metres.
- Medium: error margin between 50 and 150 metres.
- Low: error margin greater than 150 metres.
- Power consumption
- Latency (time needed for location retrieval)
- Cost
- Range of subscribers to be covered
- Availability
- Reliability

Table 2.2 displays a comparison between these positioning methods in terms of most of the aforementioned parameters.

Method	Accuracy	Latency	Availability	Reliability	Cost	Power
A-GNSS	High	< 10s (outdoors) ~ 35s	Medium	Medium	High	Medium
TDOA	Medium-Low	< 10s	Low	Medium	High	Medium
OTDOA	High-Medium	< 10s	Low	High	High	Medium
UTDOA	High-Medium	< 10s	Low	High	High	High
E-OTD	High-Medium	< 10s	Medium	Medium	Medium	Medium
AECID	Medium-Low	< 10 s	Medium	High	Medium	Medium
ECID	Low	< 5s	Medium	High	Low	Low

Table 2.2. RAN positioning methods comparison.

From Release 9 onwards, 3GPP standardized positioning techniques for LTE defining A-GNSS as the primary method, while OTDOA and ECID as the fall-back methods when satellite assisted positioning is compromised like it often happens in urban/indoors environments.

## 2.4 USSD and USSI

USSD (Unstructured Supplementary Service Data) is a GSM-based communication technology used to send text messages between mobile stations' MMI (Man Machine Interface) and applications through network entities like the USSD Gateway and the HLR.

USSD provides session-oriented communication, enabling a variety of applications. USSD messages are transferred directly over the network's signaling channels with almost null probability of traffic channel blocking even under heavy load. USSD applications can be accessed by user request through usage of short codes or text strings to trigger specific services in a session-oriented communication. These codes could perform a function, request a snippet of information, or lead the user into a series of textual menu screens which are navigated through the corresponding menu numbers.

Besides being an unstructured service, USSD has noticeable differences with SMS, namely:

- SMS is asynchronous and usually uses a “store and forward” technique to deliver text messages, meanwhile USSD is real-time session based messaging. USSD on the other hand is session oriented.
- Turnaround response times for interactive applications are up to 7 times shorter for USSD than SMS.
- USSD is not a point-to-point bearer such as SMS.
- USSD messages are limited to 182/160 bytes in length (unlike SMS, which is 160/140 bytes), where «bytes» simply mean characters depending on used encoding/language (GSM-8/7 bit encoding, Latin, Arabic, etc.).
- Establishment of Mobile Originated USSD sessions (MO USSD) requires a simple short code input at the mobile station man-machine interface (MMI).

Users do not need to access any particular menu to dial USSD short codes, which contains \* and # symbols between integer digits, always ending with «#», e.g. \*123#, \*345\*1#, #777#1#5557771234#1#.

- Applications may also start a Network Initiated USSD sessions (NI USSD) or simply USSD notifications.
- A USSD session can be initiated during a voice call.
- USSD based services work seamlessly when roaming.
- Either SIM Application Toolkit or WAP support USSD.

Some of the most popular uses for USSD are:

- Standard Supplementary Services
  - Call Forwarding
- Network Internal Services
  - Balance Inquire
  - Top-Up Prepaid Subscribers Accounts (see a call flow example in Figure 2.7).
  - Credit Transfer
- Third Party applications
  - Mobile Banking without Smartphones
  - Mobile Payments
  - Voting and Polling
  - News
  - Location Based Services

As stated before, USSD is GSM-based and its messages are embedded in MAP operations as for the SS7 protocol stack, as defined in [39-41]. For NGN like the IMS or LTE, 3GPP specified USSI (USSD for the IP Multimedia Subsystem). As there is no SS7 in these networks, USSI needed to be defined under an «all-IP» protocol to carry its payload. The chosen protocol is SIP, and the guidelines for USSD over SIP or USSI are defined by 3GPP in [42].

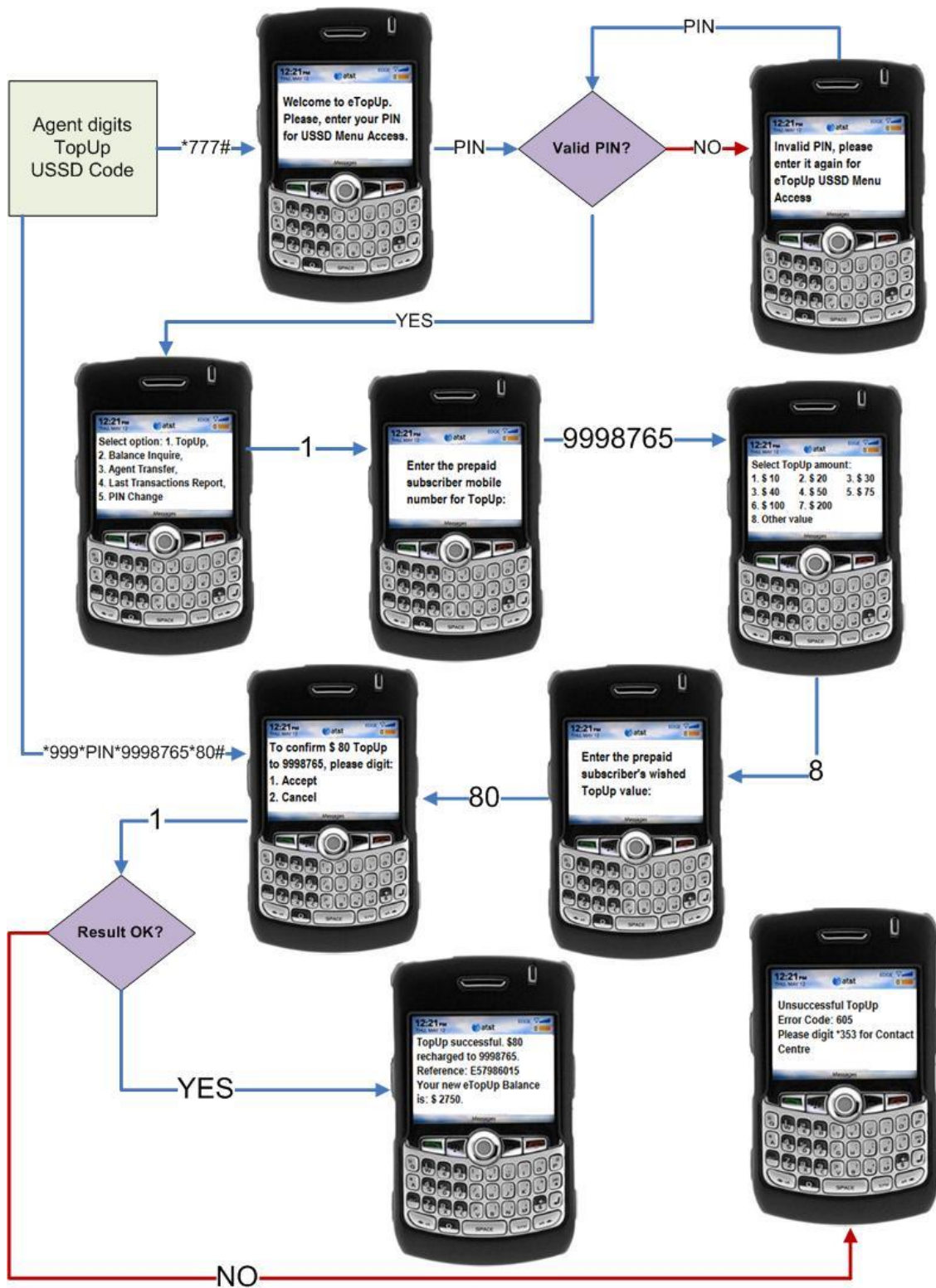


Figure 2.7. USSD call flow example of prepaid subscriber TopUp.

## Chapter 3

# 3 Open Source Framework: RestComm

## 3.1 Introduction

A modern SDP (Service Delivery Platform) may be defined as an «IT SOA Middleware», built with performance and capabilities inherent of telecommunications implementations. Figure 3.1 depicts an SDP integrated into a Telco organizational environment under the SOA paradigm [119]. Within this context, JAIN SLEE [68] Resource Adaptors (RA) have been developed to offer an abstraction of the underlying network capabilities to a Service Creation Environment (SCE). These concepts align with the first specific objective of this work, i.e.: «select an open source workspace which includes a service delivery platform, as well as network testing/simulation frameworks, with capabilities for the construction of solutions for heterogeneous telecommunication networks».

Portrayed in Figure 3.2, TeleStax' RestComm communications platforms based on Mobicents (productized as TeleStax Enterprise, e.g. TeleStax Enterprise RestComm, TeleStax Enterprise USSD Gateway, TeleStax Enterprise GMLC, etc.) are one of the industry finest examples of modern SDP or «IT SOA Middleware». Underlying network capabilities are exposed through «Enablers» which control those capabilities via JAIN SLEE RAs for either both legacy networks (MAP, CAP, etc.) or NGN (SIP, Diameter, etc.). By these means, the conjunction of adapters, enablers and Service Creation/Execution Environments (SCE/SEE), provide powerful communication abilities alike short and instant messaging services (SMS, USSD, IM, etc.), call or mobile Internet navigation control, etc., widely used in the development of multiple VAS such as subscription services, promotions, e-Wallet for payments,

transfers and remittances, emergency alerts, account balance inquiries, etc. Moreover, RAs or Web Services (REST, SOAP, XMLRPC, etc.) provide OSS/BSS smooth interworking. Hence, in-house or third parties' developments are fulfilled through the composition of enablers and/or within the SEE/SCE, independently of the underlying network technology or equipment.

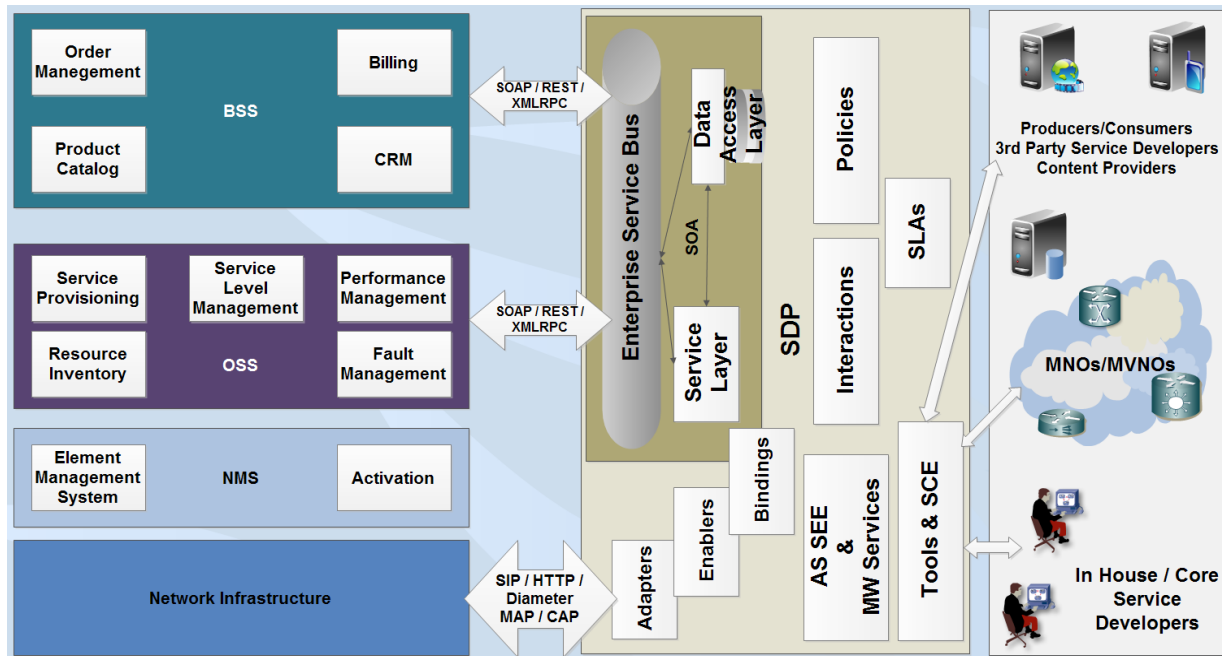


Figure 3.1. SDP integrated into a Telco organizational environment under the SOA paradigm.

Likewise, TeleStax' products are fully aligned with the aforementioned opportunity as graphically described by Alan Quayle [120] as portrayed in Figure 3.3.

TeleStax' Restcomm middleware and applications development framework allows organizations to provide a consistent, reliable and well-structured SDP that enables developers to quickly build and deploy communications applications and functionality that enhances business practices to improve internal collaboration and customer interactions.

Enterprises can then integrate additional application functionality, and ultimately migrate from costly legacy equipment and systems such as desk phones,



to softphones, mobile, soft clients, and video endpoints such as WebRTC and other communications protocols. Further, enterprises are striving to consolidate their multivendor infrastructure and integration with business applications such as; CRM, Contact Center, Collaborative Commerce and other Multi-Channel application solutions.

By integrating enhanced collaboration across its organization & applications infrastructure, organizations can enhance their communications and operational capabilities to reflect the products, resources, information, suppliers and partners necessary to develop and deliver more value. This capability management therefore depends on effective collaboration among workgroups within an organization, and its partners and suppliers outside of it. TeleStax eliminates bifurcated communications silos while enabling its customers to decouple services from the network infrastructure, thus enabling voice, video, and collaboration services to operate efficiently and independently.

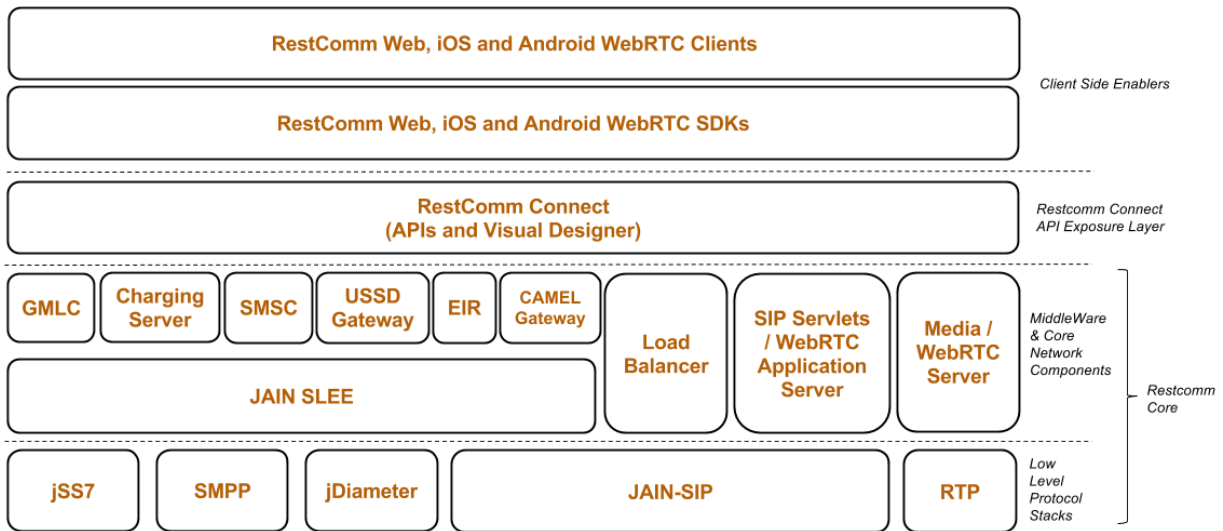


Figure 3.2. TeleStax RestComm Communication Platform architecture based on Mobicents.

## 3.2 Features

- Built on top of Carrier Grade Mobicents Platform:
  - JAIN SLEE, WebRTC and SIP Servlets.
  - Compliant with both legacy networks communication protocols over SS7/SIGTRAN (GSM, GRPS/EDGE, UMTS/HSPA+) and NGN (LTE and the IMS) all-IP based protocols (SIP, Diameter, etc.). Therefore, ready for VAS for either legacy GSM/UMTS or IMS/LTE/IoT.
- Telecom API for Web Developers, agnostic of underlying Telecom infrastructure.
  - RestComm Visual Designer tool providing Drag & Drop office users and Copy & Paste weekend developers as their SCE.
- RestComm Mobile Application App Store.
- Deployable in public/private/hybrid clouds.
- Pluggable architecture, designed for scalability.
- Offers 100% API Compatibility with Twilio®
- Voice/SMS/USSD/MMS/ASR/TTS/LBS service provider agnostic.

RestComm is already successfully integrated with Project Clearwater [121], an Open Source implementation of IMS designed from the ground up for massively scalable deployment in the Cloud to provide voice, video and messaging services. Its cloud oriented design makes it extremely well suited for deployment in a NFV environment. Therefore, CSPs still with no IMS deployments, or research NGN/IMS laboratories such as University of Cauca's «Telco 2.0» project, might find this TeleStax partnership as a step forward into NGN full compliance either on networking

capabilities or paradigm shifts towards ICT new trends (e.g. SOA, SDN, NFV, IoT, etc.).

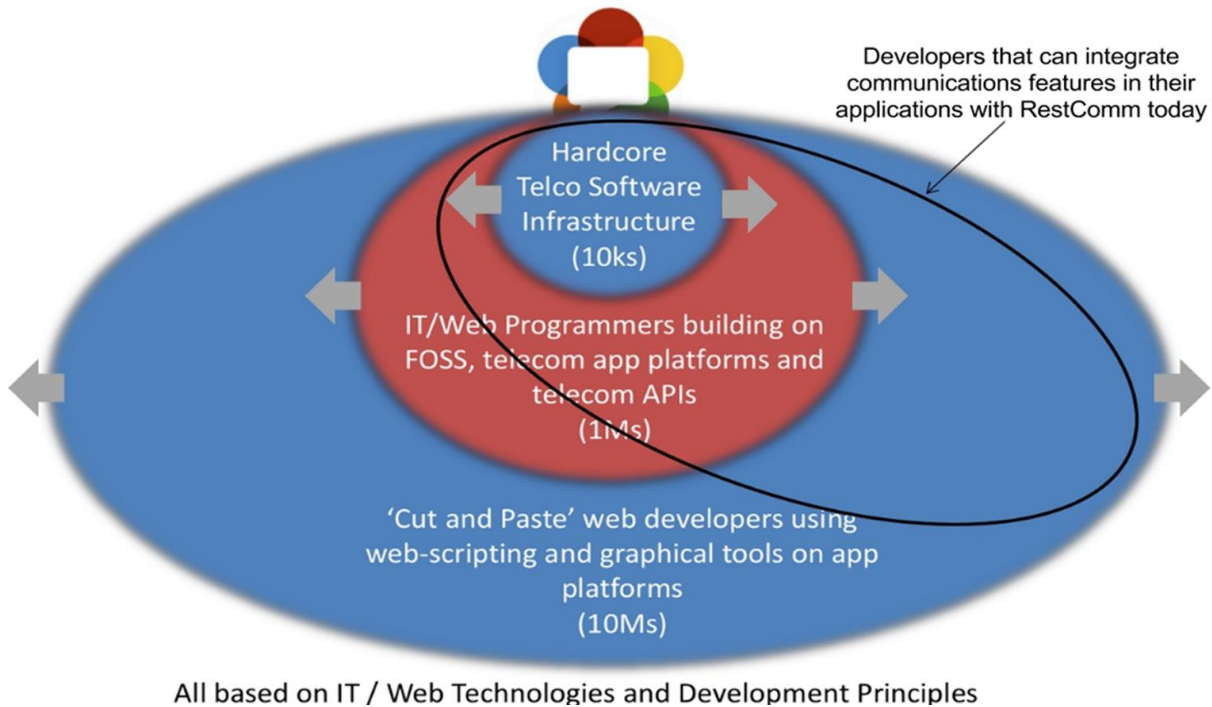


Figure 3.3. TeleStax' RestComm opportunity offer to CSPs (source: Alan Quayle [120]).

### 3.3 USSD and SMSC Gateways

USSD Gateway provides core features either for Mobile Originated and Mobile Initiated USSD messages either over SS7 based Circuit-Switched Core Networks (via SIGTRAN or legacy E1 links) and also provides translation capabilities to IP based protocols like SIP (according to 3GPP technical specification for USSD for the IP Multimedia Subsystem [42]) or HTTP, either for RestComm or third parties processing through Web Services (REST, SOAP, XMLRPC, etc.).

Figure 3.4 portrays an example USSD message sequence a User Equipment starting a TeleStax Enterprise USSD Gateway, RestComm SIP Servlets and a third-party application. This example assumes that third-party application sends back tree based menu via HTTP means.

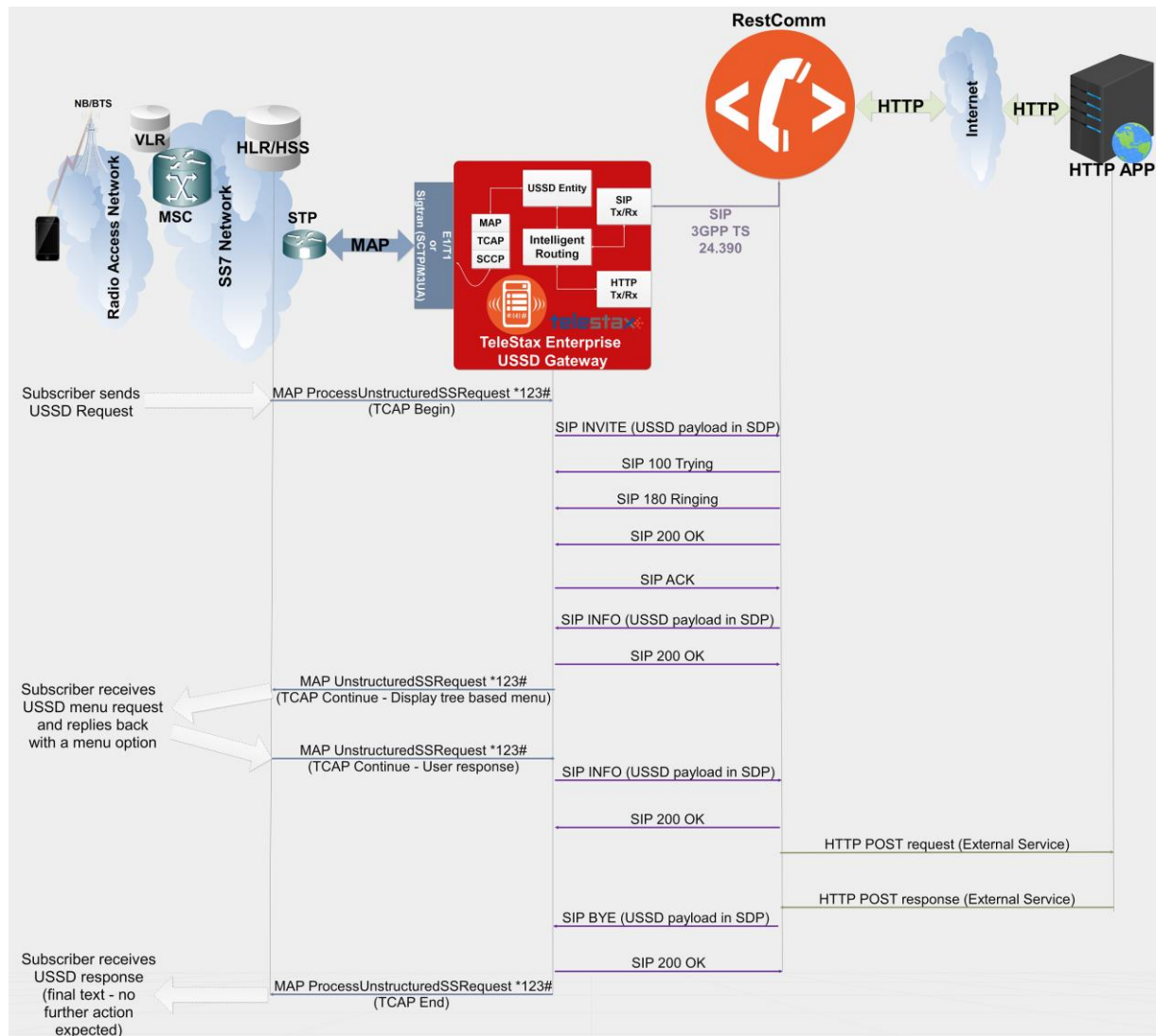


Figure 3.4. Signal flow example of Mobile Originated USSD session established with third party application throughout TeleStax Enterprise RestComm across SS7 and IP-based networks (Annex E provides a trace for such example).

TeleStax Enterprise SMSC Gateway provides core features for SMS messaging (either for Mobile Originated and Mobile Initiated SMS either over SS7 based Circuit-Switched Core Networks with Store and Forward capabilities, translation capabilities to IP based protocols for Instant Messaging (IM through SIP), HTTP and SMPP either for RestComm or third parties processing. Additionally, it provides among other features out of scope of this document, Diameter Credit Control with Online Charging System (DCCA/Ro Interface).

Figure 3.5 displays a signal flow example of an incoming SMS from SS7 over MAP, routed from RestComm SMSC to RestComm SIP Servlets over SIP and delivered to third party HTTP Application.

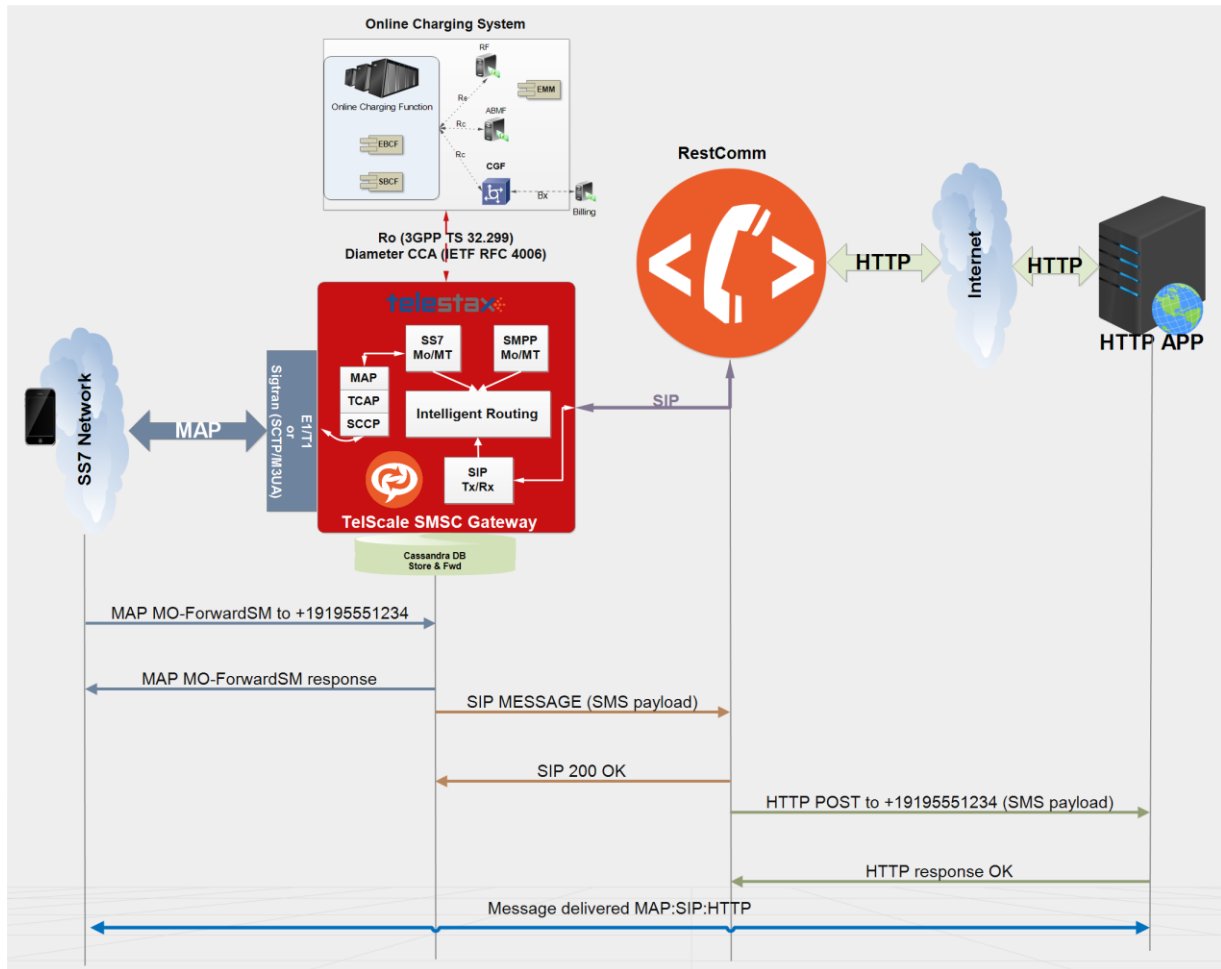


Figure 3.5. Signal flow example of Mobile Originated SMS delivery to third party application throughout RestComm across SS7 and IP-based networks.

Likewise, either TeleStax Enterprise SMSC or TeleStax Enterprise USSD Gateways are capable of processing SMS either over legacy SS7 based Circuit-Switched Core Networks or NGN such as LTE/LTE Advanced and the IMS. Messages crossing entities from both scenarios are covered, as a MAP based flow can be supported in the meantime SIP Application Servers at the IMS control it, along with IMS' CSCFs or HSS and LTE's EPC entities such as P-GW, S-GW, and PCRF

might be involved in the corresponding SIP conversational state. Please refer to Annex E for a detailed example on this regard, specifically for USSD and USSI.

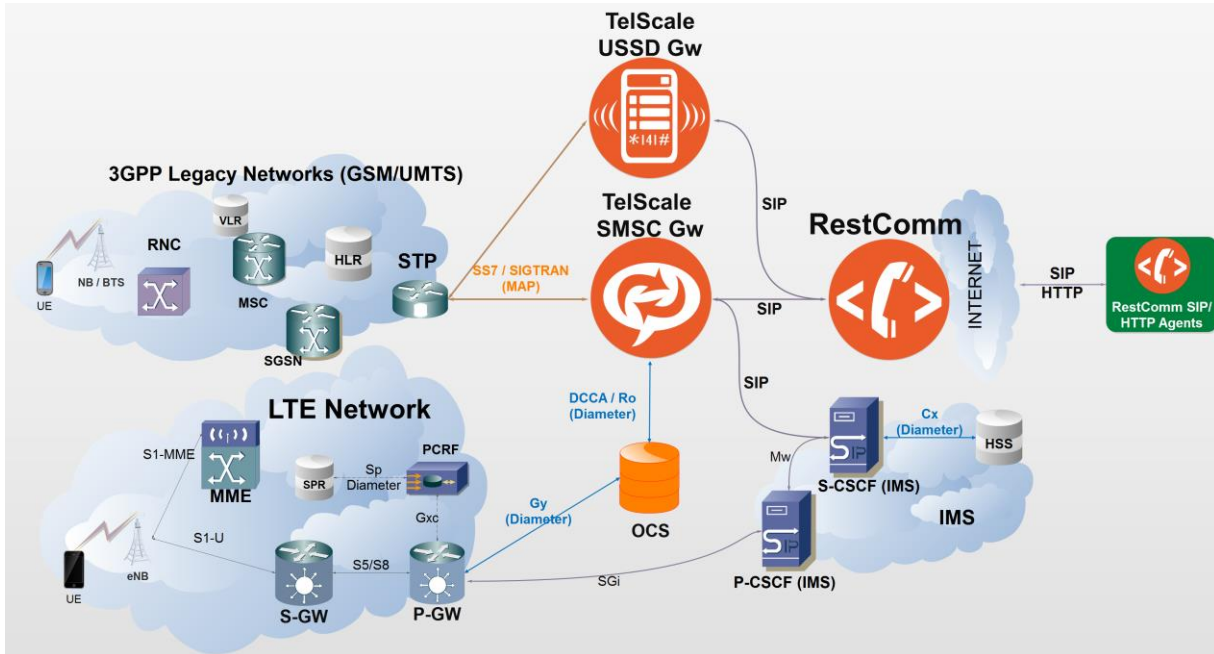


Figure 3.6. TeleStax Enterprise RestComm, SMSC and USSD Gateways interworking among heterogeneous networks.

### 3.4 Other Components

RestComm jDiameter offers client and server side suite of services and tools for the Diameter family of protocols. It implements Diameter base protocol [31] as well as some of the most important and widely used Diameter applications (DCCA, Ro, Rf, Sh, Cx/Dx, Gq', Gx, Rx, S6a), allowing a fast development of LTE/4G and IMS components and interfaces such as the ones between SIP Application Server (AS), Call Session Control Function (CSCF) and Home Subscriber Server (HSS) or Subscriber Location Function (SLF). jDiameter is extensible to provide support for additional Diameter applications.

RestComm Mobile Client SDKs provide programming interfaces to add communication capabilities to mobile Apps, i.e. WebRTC audio & video calls or text

messages. Provide easy to use APIs for iOS and Android. Client SDKs connect to RestComm platform to take advantage of its communications features. Depending on the RestComm application logic, a wealth of possibilities opens up, namely:

- ✓ Calls to PSTN or Mobile User Equipment;
- ✓ SMS to Mobile Networks;
- ✓ P2P (Peer to Peer) audio & video calls and text messages to other RestComm Client endpoints (both mobile and Web), either over cellular or WiFi radio access (see Figure 3.6);



Figure 3.7. LTE video call via RestComm iOS/Android SDK.

TeleStax Enterprise GMLC, prior to this work, only supported OMA's MLP interface with GMLC clients for mobile location retrieval through SS7 MAP ATI operation.

Other TeleStax communication products are out of the scope of this work, thus are not covered in this document. Figure 3.8 displays TeleStax' RestComm/TeleStax Enterprise communication platforms across the Internet and Mobile Core and Radio



Access Networks of all generations up to date. SL<sub>g</sub> interface between TeleStax Enterprise GMLC and the MME (ELP Diameter) as well as MLP/SIP interface between RestComm and TeleStax Enterprise GMLC were missing until this work was offered as a contribution aligned with TeleStax Open Source Playbook [122].

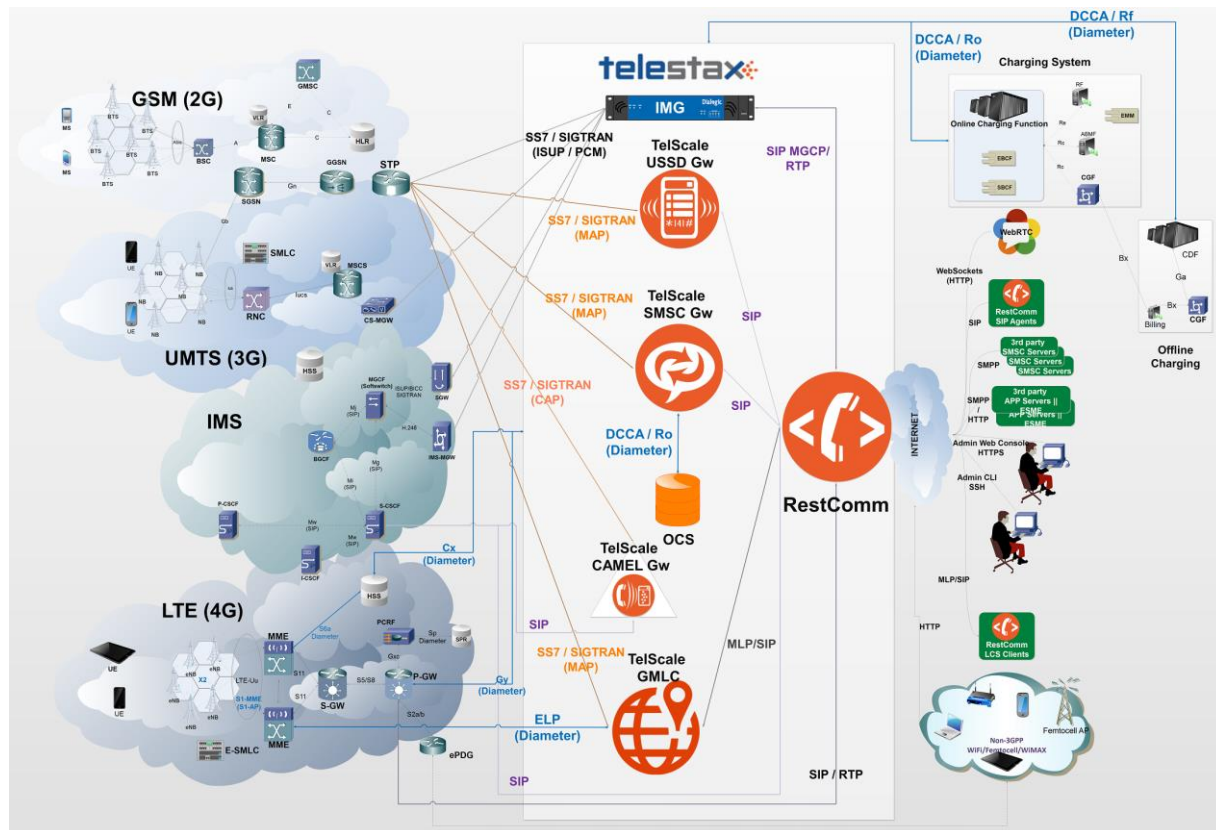


Figure 3.8. TeleStax' communication platforms integrated to MNO Core Networks from GSM to LTE.

### 3.5 Conclusion

Given all the facts covered thus far throughout this chapter, TeleStax' RestComm/TeleStax Enterprise (also called TelScale) communication platforms and simulation tools fulfils the goals included within the first specific objective of this work.



## Chapter 4

### 4 RestComm Geolocation API

RestComm Geolocation API has been designed and developed for satisfying the motivational scenarios introduced earlier in this document (as well as other purposes that surged from further internal brainstorming, the open source community interaction with colleagues from TeleStax partners and customers, TADHack organization, the Illinois Institute of Technology at TADHack-mini Chicago 2015 event, etc.), by providing Web or Mobile developers a «SOA» approach interface for performing location services in all kinds of wireless networks.

RestComm RESTful APIs comprise a set of web service endpoints that allows managing and using RestComm resources through the standard HTTP methods. Likewise, it features the following:

- creating, reading, updating and deleting accounts, phone numbers, calls, text messages, recordings, etc.;
- creating and controlling Voice, SMS and USSD sessions (start a new call, send a new SMS message, etc.), and beyond this project, geolocation services;
- secured access through authentication, HTTPS protocol and Multi-tenancy control.

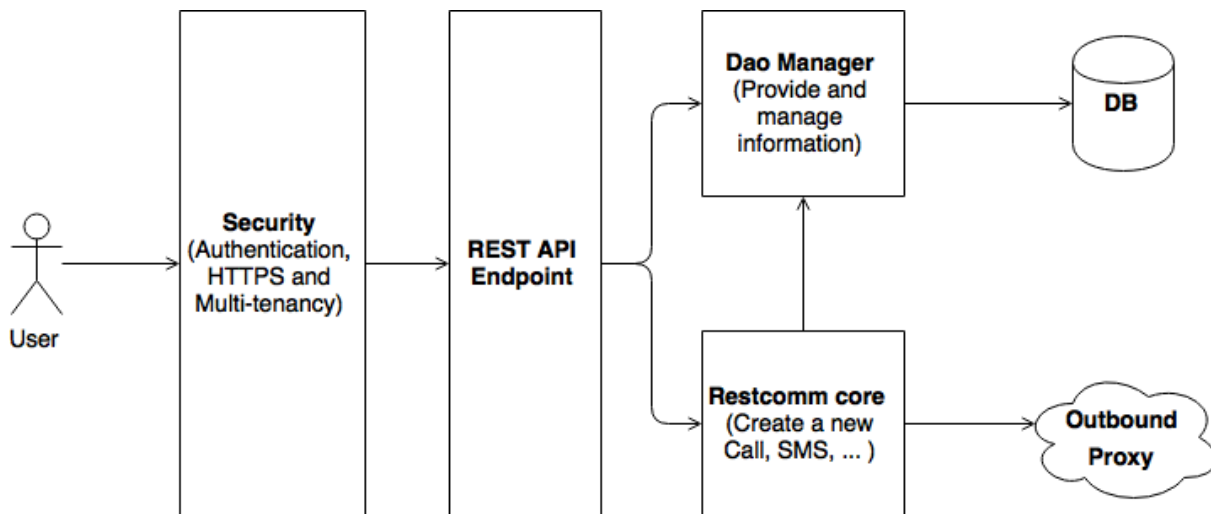


Figure 4.1. RestComm API's simple access diagram.

Figure 4.2 portrays an UML overview of RestComm Geolocation API endpoint structure.

Following, a brief description of RestComm Geolocation API REST API Endpoint structure classes (graphically shown in Figure 4.2):

- **AbstractEndpoint:** holds the common structure used by all endpoints.
- **SecuredEndpoint:** Security layer endpoint which scans requests for security related assets and populate the user identity context accordingly.
- **GeolocationEndpoint:** implements RestComm Geolocation API endpoint logic.
- **GeolocationXmlEndpoint:** links HTTP methods with RestComm Geolocation API endpoint logic through XML.
- **GeolocationJsonEndpoint:** links HTTP methods with RestComm Geolocation API endpoint logic through JSON.
- **AbstractConverter:** holds the common structure for building all responses.
- **GeolocationConverter:** implements creation of specific JSON and XML responses.
- **GeolocationDao:** interface to access and interact with MyBatis database layer.

- **Geolocation**: entity class defining a **Geolocation resource**, which can be either of type «**Immediate**» or «**Notification**» (classified under the enumeration attribute «**GeolocationType**»).

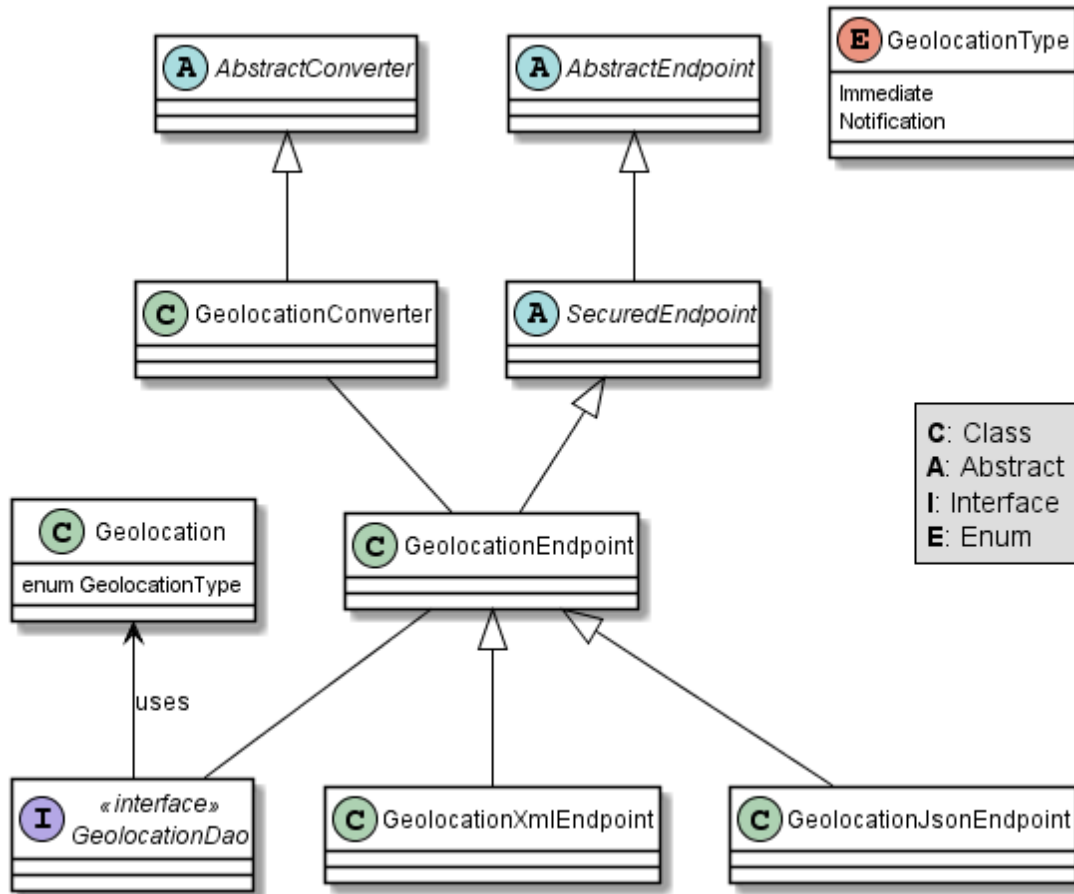


Figure 4.2. RestComm Geolocation API REST API Endpoint structure.

RestComm Geolocation API aims offering an API that Web Developers can understand without the need of any knowledge about the underlying Telecom infrastructure and jargon and thus make it as easy as it gets to include Geolocation as a value-added feature in their applications. The API aims to cater either cellular telephony Geolocation (from Mobile Network Operator’s core and radio access networks, either by SS7 MAP or LTE Diameter operations) or IP Geolocation (from Restcomm iOS and Android SDKs). Some use cases this API intends covering are:

- Notify RestComm the current location of client X or certain MSISDN (e.g. iWatch cardio activity alarm –2015 TADHack Chicago winner- [125], NG911 [105], friend/family finder, etc.).
- Notify RestComm if client X or certain MSISDN enters or exits a geofence. Mobile advertising use cases apply to this type of Geolocation service.
- Notify RestComm if client X is within N meters from client Y. Many use cases apply to this type of Geolocation service, namely:
  - Parental control: Notify a parent when their child/children are further than X metres away.
  - Hanging out: Notify friends when they are within X metres.
  - Business matching: at a conference, notify attendees of other attendees within range who also have related interest based on LinkedIn profile.
  - Court restraining order: when someone is legally not allowed to be within certain range of another individual.

Further use cases will be covered in future iterations of the API based on community and TeleStax' customer feedback.

## 4.1 Geolocation Resource

A Geolocation resource represents an outbound Geolocation service.

### 4.1.1 Geolocation Resource URI

Geolocation Resource URI distinct in three modes described further below:

**`/ApiVersion/Accounts/{AccountSid}/Geolocation/{GeolocationSid}`**

This URI refers to requests that would only allow HTTP GET method to retrieve previously gathered Geolocation information, regardless of whether it was an Immediate or Notification Geolocation request (see further below for description of those terms).

#### 4.1.2 Geolocation Resource Properties

PROPERTY	DESCRIPTION
Sid	A string that uniquely identifies this Geolocation service.
DateCreated	The date that this Geolocation service was created.
DateUpdated	The date that this Geolocation service was last updated.
DateExecuted	The date that this Geolocation service was executed.
AccountSid	A string that uniquely identifies the account that created this Geolocation service.
Source	A string that uniquely identifies the Geolocation service client, phone number or device that initiated the Geolocation service.
DeviceIdentifier	A string that uniquely identifies the device target (e.g. phone number, IoT device) of this Geolocation service.
GeolocationType	<p>The type of location measurement requested, namely:</p> <p><b>Immediate:</b> after a successful geolocation request has been delivered with its associated timestamp, the location information and timestamp are referred to as the 'current location' at that point in time.</p> <p><b>Notification:</b> location request where the response/s is/are required after a specific event has occurred. Event may or may not occur immediately. In addition, event may occur many times. Examples of these events: when a device is entering, leaving or being in a pre-defined geographical area (geofencing); periodic location; when a device becomes available; when a sensor/beacon detects a threshold surpassed, etc.</p>
ResponseStatus	<p>A string that uniquely identifies the current state of this Geolocation service. Possible values are:</p> <p><b>queued:</b> whenever the location request is buffered due</p>

	<p>to abnormal causes (e.g. congestion at the GMLC);</p> <p><b>sent:</b> when the location request has already been sent but no response has arrived yet;</p> <p><b>processing:</b> when the location response has been received, but being under computational process for delivery to the requesting location client.</p> <p><b>successful:</b> when the location response has been received, and processed with complete fulfilment of quality of geolocation information.</p> <p><b>partially-successful:</b> when the location response has been received and processed, but not fulfilled the whole set of geolocation information or desired accuracy, e.g.: geographic coordinates were not possible to retrieve, but at least other location information such as Cell and Location Area identifiers were obtained; location information was retrieved, but the age of location estimate denotes it may be outdated; location information was retrieved, but informed that precision is not reliable due to high error margin.</p> <p><b>last-known:</b> when location information could not be retrieved from the network but there is a previous persisted location information for the targeted '<i>DeviceIdentifier</i>' of this Geolocation service.</p> <p><b>failed:</b> when location information could not be retrieved from the network and there's no previous location information persisted for the targeted '<i>DeviceIdentifier</i>' of this Geolocation service, or when an attempt to update this Geolocation service was malformed or not</p>
--	---

	<p>API compliant. In the latter situation, the record persists, but previous geolocation information is erased (expecting a correct geolocation update).</p> <p><b>unauthorized:</b> when the location request is or has become disallowed from the network, the location client requesting this service is not authorized for such operation or the target device is marked for not authorizing this kind of location requests. A record is persisted for security and analytics purposes.</p> <p><b>rejected:</b> when the location request does not meet the API's requirements for mandatory parameters (or some of them are missing), or prohibited parameters are included for a certain type of Geolocation. No records are persisted in this eventuality.</p>
GeolocationData	<p>An array that uniquely identifies the location information that might be obtained by this Geolocation service. The fields of this array are described next:</p> <p><b>CellId:</b> an identifier assigned to a specific radio coverage area known as cell;</p> <p><b>LocationAreaCode:</b> an identifier assigned to a group of cells;</p> <p><b>MobileCountryCode:</b> code number of the country of the mobile network as specified by E.212.</p> <p><b>MobileNetworkCode:</b> code number of the mobile network in a specific country as specified by E.212.</p> <p><b>NetworkEntityAddress:</b> code number of the mobile network entity addressed for this Geolocation service.</p>

	<p><b>LocationAge:</b> indication of how long ago the network location identifiers were recorded (informed in minutes);</p> <p><b>DeviceLatitude:</b> an estimate of the location of the phone number, device/beacon or closest WiFi Access Point in the geographic coordinate that specifies the north-south position of a point on the Earth's surface. WGS84 is used, whose formats for Latitude are described next. Latitude valid formats include:</p> <p>N43°38'19.39" 43°38'19.39"N 43 38 19.39 43.63871944444445</p> <p>If expressed in decimal form, northern latitudes are positive, southern latitudes are negative. The following longitude variants are also allowed:</p> <p>N43 38 19.39 43 38 19.39N</p> <p><b>DeviceLongitude:</b> an estimate of the location of the phone number, device/beacon or closest WiFi Access Point in the geographic coordinate that specifies the north-south position of a point on the Earth's surface. WGS84 is used, whose formats for Longitude are described next. Longitude valid formats include:</p> <p>W116°14'28.86" 116°14'28.86"W -116 14 28.86 -116.2413513485235</p> <p>If expressed in decimal form, eastern longitudes are positive, western longitudes are negative. The following longitude variants are also allowed:</p> <p>W116 14 28.86 116 14 28.86W</p>
--	---



	<p><b>Accuracy:</b> quality of location information or estimated precision for this Geolocation service in meters. This information will be present depending on available location procedures at the radio access network.</p> <p><b>PhysicalAddress:</b> MAC address of the device/beacon or closest WiFi Access Point.</p> <p><b>InternetAddress:</b> IP address of the phone number, device/beacon or closest WiFi Access Point.</p> <p><b>FormattedAddress:</b> refers to the civic location of the phone number, device/beacon or closest WiFi Access Point, expressed as civic data (e.g. floor, street number, city.) It shall be represented in a well-defined universal format, compliant with Google Geolocation API's "formatted_address" json/xml field.</p> <p><b>LocationTimestamp:</b> indication of when the geolocation information was gathered (informed as a time stamp);</p> <p><b>EventGeofenceLatitude:</b> refers to the geographic coordinates' latitude of a specific location. Used to notify when a device is within a certain distance (in metres) from that specific location. Some format used as for "DeviceLatitude" parameter.</p> <p><b>EventGeofenceLongitude:</b> refers to the geographic coordinates' longitude of a specific location. Used to notify when a device is within a certain distance (in metres) from that specific location. Some format used as for "DeviceLongitude" parameter.</p> <p><b>Radius:</b> distance in meters from the Geofence</p>
--	--

	geographic coordinates.
GeolocationPositioningType	<p>Indication of the positioning method used to determine the Geolocation data, either successfully or unsuccessfully. Possible values are:</p> <p><b><i>last-known</i></b>: last known device location position stored at a database (Location Server, HLR, etc.) from which the information is retrieved.</p> <p><b><i>Network</i></b>: location information retrieved from improved measurement techniques executed at the radio access network, either for IP or cellular networks (e.g. timing advanced, multilateration, etc.).</p> <p><b><i>GPS</i></b>: location information assisted by the Global Navigation Satellite System (GNSS), which includes GPS (as well as GLONASS and Galileo).</p>
LastGeolocationResponse	Indication whether “GeolocationData” values provided are the last to be gathered in this Geolocation request (true/yes) or further are expected to be sent asynchronously (false/no) to the “StatusCallback” URL.
Cause	Reason of an unsuccessful or rejected Geolocation request.
ApiVersion	The API version RestComm used to handle the Geolocation service.
Uri	The URI for this account, relative to <code>http://localhost:port/restcomm</code> .

Table 4.1. RestComm Geolocation API resource properties.

### 4.1.3 Supported Operations

**HTTP GET.** Returns the list representation of all the service resources for the account, including the properties listed in Table 4.1.

## 4.2 Immediate Geolocation

### 4.2.1 Immediate Geolocation URI

**`/ApiVersion/Accounts/{AccountSid}/Geolocation/Immediate/{GeolocationSid}`**

This URI mode refers to requests for retrieval of current or last known Geolocation information (an associated timestamp will be included in the response). Geolocation information might include very accurate location data in terms of geographic coordinates, or just location identifiers like the radio base station transceiver identity of a cellular network that is currently providing service to the target device. Accuracy will depend on the available radio access location procedures, either within a Mobile Network Operator for mobile handsets location within a cellular Radio Access Network, or a WLAN/WiFi covered area for IP location.

### 4.2.2 Immediate Geolocation supported operations

**HTTP GET.** Returns the list representation of all the service resources for this account, including the aforementioned properties.

**HTTP POST.** Sends a new location request and returns the representation of the Location request resource, including the aforementioned properties.

**HTTP PUT.** Updates an Immediate Geolocation request and returns the representation of the Geolocation request resource, including the aforementioned properties.

**HTTP DELETE.** Stops an Immediate Geolocation request previously created or updated.

### 4.2.3 Immediate Geolocation list of required parameters

PARAMETER	DESCRIPTION
DeviceIdentifier	The target E.164 phone number or device identity of this Geolocation service.
StatusCallback	A URL that RestComm will use when the Geolocation service reaches a state that demands notifying the requesting application. Note: Typically, if the Geolocation request is using Low Accuracy, the Geolocation information can be retrieved quickly, thus the result may be returned synchronously. For more precise accuracy, it will take longer to gather the Geolocation information, as such this URL will be called back (potentially multiple times) as the Geolocation information is gathered.

Table 4.2. Immediate Geolocation list of required parameters.

### 4.2.4 Immediate type of Geolocation examples

#### 4.2.4.1 Immediate Geolocation of a specific IP device associated to a User; Partial and Successful answers, whole Status Callback cycle example

A curl example for a Geolocation request originated from a mobile (iOS or Android) location client is shown next. This Geolocation service assumes WiFi connection only, thus the location information is obtained from an Access Point (AP) management system, typically placed in indoors surroundings like shopping centers, theaters, domes, etc. In the first instance, the Location Server cannot determine a precise location information, responding back with the last known location. Later, best available accuracy is processed and informed back to the corresponding Status Callback URL.

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate -d
```

```
"DeviceIdentifier=client:david" -d
"StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response below for a partially-successful positioning procedure is shown next:

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50271</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:36:12 -0500</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>client:david</DeviceIdentifier>
    <GeolocationType>immediate</GeolocationType>
    <ResponseStatus>partially-successful</ResponseStatus>
    <GeolocationData>
      <DeviceLatitude>33.786442</DeviceLatitude>
      <DeviceLongitude>-84.38103</DeviceLongitude>
      <PhysicalAddress>00-41-76-C0-00-D1</PhysicalAddress>
      <InternetAddress>65.17.24.177</InternetAddress>
      <FormattedAddress>187 14th St NE Atlanta, GA 30309-2674,
      USA</FormattedAddress>
      <LocationTimestamp>Mon, 25 Jan 2016 16:36:12 -0500</LocationTimestamp>
    </GeolocationData>
    <GeolocationPositioningType>last-known</GeolocationPositioningType>
    <LastGeolocationResponse>>false</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354
440b09213d04752f50271</Uri>
  </Geolocation>
</RestcommResponse>
```

The corresponding status callback after a network measurement updated the previously stored last known location data is shown next (still a partially-successful positioning procedure though, desired accuracy is not accomplished yet):

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50271</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:36:25 -0500</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>client:david</DeviceIdentifier>
    <GeolocationType>immediate</GeolocationType>
    <ResponseStatus>partially-successful</ResponseStatus>
    <GeolocationData>
      <DeviceLatitude>33.770002</DeviceLatitude>
```

```

    <DeviceLongitude>-84.5200998</DeviceLongitude>
    <Accuracy>150</Accuracy>
    <PhysicalAddress>00-41-76-C0-00-D1</PhysicalAddress>
    <InternetAddress>65.17.21.37</InternetAddress>
    <FormattedAddress>37 5th St NE Atlanta, GA 30310-2179,
USA</FormattedAddress>
    <LocationTimestamp>Mon, 25 Jan 2016 16:36:25 -0500</LocationTimestamp>
  </GeolocationData>
  <GeolocationPositioningType>Network</GeolocationPositioningType>
  <LastGeolocationResponse>>false</LastGeolocationResponse>
  <ApiVersion>2012-04-24</ApiVersion>
  <Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354
440b09213d04752f50271</Uri>
</Geolocation>
</RestcommResponse>

```

Finally, the corresponding response below for the successful positioning procedure informed in a posterior status callback when high accuracy is accomplished through GPS assistance is displayed next:

```

<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50271</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:38:24 -0500</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>client:david</DeviceIdentifier>
    <GeolocationType>immediate</GeolocationType>
    <ResponseStatus>partially-successful</ResponseStatus>
    <GeolocationData>
      <DeviceLatitude>33.870042</DeviceLatitude>
      <DeviceLongitude>-84.5190103</DeviceLongitude>
      <Accuracy>5</Accuracy>
      <PhysicalAddress>00-41-76-C0-00-D1</PhysicalAddress>
      <InternetAddress>65.17.21.37</InternetAddress>
      <FormattedAddress>34 5th St NE Atlanta, GA 30310-2178,
USA</FormattedAddress>
      <LocationTimestamp>Mon, 25 Jan 2016 16:38:24 -0500</LocationTimestamp>
    </GeolocationData>
    <GeolocationPositioningType>GPS</GeolocationPositioningType>
    <LastGeolocationResponse>true</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354
440b09213d04752f50271</Uri>
  </Geolocation>
</RestcommResponse>

```

#### 4.2.4.2 Geolocation of a specific Mobile device associated to a phone number; response including geographic coordinates

A curl example for a Geolocation request originated initiated by E.164 phone number 59899549878 requesting location information of E.164 phone number 59897018375 is displayed next. This case assumes that the Geolocation information is retrieved successfully from a cellular network with capabilities for obtaining geographic coordinates (multilateration with at least three base stations) as well as core and radio access network identifiers.

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate -d
"DeviceIdentifier=59897018375" -d
"StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response is shown next.

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50272</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0300</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:37:21 -0300</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0300</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>59897018375</DeviceIdentifier>
    <GeolocationType>immediate</GeolocationType>
    <ResponseStatus>successful</ResponseStatus>
    <GeolocationData>
      <CellId>90183B</CellId>
      <LocationAreaCode>751</LocationAreaCode>
      <MobileCountryCode>748</MobileCountryCode>
      <MobileNetworkCode>01</MobileNetworkCode>
      <NetworkEntityAddress>59800023041</NetworkEntityAddress>
      <LocationAge>0</LocationAge>
      <DeviceLatitude>-34.541079</DeviceLatitude>
      <DeviceLongitude>-56.1421274</DeviceLongitude>
      <Accuracy>50</Accuracy>
      <LocationTimestamp>Mon, 25 Jan 2016 16:37:21 -0300</LocationTimestamp>
    </GeolocationData>
    <GeolocationPositioningType>Network</GeolocationPositioningType>
    <LastGeolocationResponse>true</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354
440b09213d04752f50272</Uri>
  </Geolocation>
</RestcommResponse>
```

#### 4.2.4.3 Geolocation of a specific Mobile Device associated to a phone number; no geographic coordinates included in response

A curl example for a Geolocation request originated from an application called “eTop” requesting location information of E.164 phone number 59897018375 is displayed next. This case assumes that the Geolocation information is retrieved from a cellular network, but in contrast with the example described in section 4.2.4.1, with no capabilities for obtaining geographic coordinates but at least core and radio access network identifiers are available (typical of 2G cellular networks).

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate -d
"DeviceIdentifier=39897018375" -d
"StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response is portrayed next.

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50273</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 +0200</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:36:11 +0200</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 +0200</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>39897018375</DeviceIdentifier>
    <GeolocationType>immediate</GeolocationType>
    <ResponseStatus>partially-successful</ResponseStatus>
    <GeolocationData>
      <CellId>19012A</CellId>
      <LocationAreaCode>901</LocationAreaCode>
      <MobileCountryCode>222</MobileCountryCode>
      <MobileNetworkCode>48</MobileNetworkCode>
      <NetworkEntityAddress>3980000101</NetworkEntityAddress>
      <LocationAge>0</LocationAge>
      <LocationTimestamp>Mon, 25 Jan 2016 16:36:11 +0200</LocationTimestamp>
    </GeolocationData>
    <GeolocationPositioningType>Network</GeolocationPositioningType>
    <LastGeolocationResponse>true</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354
440b09213d04752f50273</Uri>
  </Geolocation>
</RestcommResponse>
```



#### 4.2.4.4 Geolocation of a specific IP device associated to a user: Failed execution response

A curl example for a Geolocation request originated from a mobile (iOS or Android) location client, exactly like the latest example, but on this occasion with a 'failed' result (e.g. no geographic coordinates or civic address could be obtained from the AP management system) is depicted next.

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate -d
"DeviceIdentifier=sip:david@65.17.24.177" -d
"StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response is displayed below.

```
<RestcommResponse>
<Geolocation>
  <Sid>GLfa51b104354440b09213d04752f50274</Sid>
  <DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
  <DateUpdated>Mon, 25 Jan 2016 16:36:37 -0500</DateUpdated>
  <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
  <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
  <DeviceIdentifier>sip:david@65.17.24.177</DeviceIdentifier>
  <GeolocationType>immediate</GeolocationType>
  <ResponseStatus>failed</ResponseStatus>
</GeolocationData>
<Cause>Timeout, no response from network</Cause>
<ApiVersion>2012-04-24</ApiVersion>
<Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354
440b09213d04752f50274</Uri>
</Geolocation>
</RestcommResponse>
```

It is important to note that records are persisted when ResponseStatus equals "failed", thus they could be updated by a further operation, a POST or PUT request, or retrieved by a GET request.

#### 4.2.4.5 Geolocation update of a previously failed request

A curl example for updating the previous Geolocation request example is encompassed next. In this case, the last known location is set instead of the empty location data response obtained previously due to a network failure.

```
curl -X PUT -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:f8bc1274677b173d1a1cf3b9924eaa7e@192.168.118.134:8080/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354440b09213d04752f50274 -d "DeviceLatitude=43.257134" -d "DeviceLongitude=-3.496932" -d "LocationTimestamp=2016-01-17T20:32:28.488-04:00" -d "PhysicalAddress=D8-97-BA-19-02-D8" -d "InternetAddress=2001:0:9d38:6ab8:30a5:1c9d:58c6:5898" -d "LastGeolocationResponse=false" -d "GeolocationPositioningType=last-known"
```

The corresponding response is displayed next.

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50274</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 20:40:10 -0500</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>sip:david@65.17.24.177</DeviceIdentifier>
    <GeolocationType>Immediate</GeolocationType>
    <ResponseStatus>last-known</ResponseStatus>
    <GeolocationData>
      <DeviceLatitude>35.669860</DeviceLatitude>
      <DeviceLongitude>-81.22147</DeviceLongitude>
      <InternetAddress>2001:0:9d38:6ab8:30a5:1c9d:58c6:5898</InternetAddress>
      <PhysicalAddress>D8-97-BA-19-02-D8</PhysicalAddress>
      <LocationTimestamp>Sun, 17 Jan 2016 21:32:28 -0500</LocationTimestamp>
    </GeolocationData>
    <GeolocationPositioningType>last-known</GeolocationPositioningType>
    <LastGeolocationResponse>false</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354440b09213d04752f50274</Uri>
  </Geolocation>
</RestcommResponse>
```

#### 4.2.4.6 Gathering information of a specific previously satisfactory created Geolocation Request

A curl example of retrieving the information of the Geolocation service request from the previous example is portrayed next.

```
curl -X GET
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0.1:8080/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354440b09213d04752f50274
```

The corresponding JSON response is shown below (the XML response would be exactly as displayed previously for the POST request).

```
{
  "sid": "GLfa51b104354440b09213d04752f50274",
  "date_created": "Mon, 25 Jan 2016 16:36:10 -0500",
  "date_updated": "Mon, 25 Jan 2016 20:40:10 -0500",
  "date_executed": "Mon, 25 Jan 2016 16:36:10 -0500",
  "account_sid": "ACae6e420f425248d6a26948c17a9e2acf",
  "device_identifier": "sip:david@65.17.24.177",
  "geolocation_type": "Immediate",
  "response_status": "last-known",
  "geolocation_data": {
    "device_latitude": "35.669860",
    "device_longitude": "-81.22147",
    "internet_address": "2001:0:9d38:6ab8:30a5:1c9d:58c6:5898",
    "physical_address": "D8-97-BA-19-02-D8",
    "location_timestamp": "Sun, 17 Jan 2016 21:32:28 -0500"
  },
  "geolocation_positioning_type": "last-known",
  "last_geolocation_response": "false",
  "api_version": "2012-04-24",
  "uri": "/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate/GLfa51b104354440b09213d04752f50274.json"
}
```

#### 4.2.4.7 Rejected Immediate Geolocation request

Following, a curl example for a Geolocation request originated from a RestComm Location Client, but on this occasion with a 'rejected' result as a mandatory parameter is missing:

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0.1:8080/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Immediate -d "DeviceIdentifier=4498750163"
```

This request gets an HTTP/1.1 400 Bad Request response with following text:  
StatusCallback value cannot be null

No records are persisted for HTTP/1.1 400 Bad Request responses. Hence, they cannot be updated by either a further POST or PUT request, or retrieved through a GET request.

## 4.3 Notification Geolocation

### 4.3.1 Notification Geolocation URI

**`/ApiVersion/Accounts/{AccountSid}/Geolocation/Notification/{GeolocationSid}`**

This URI mode refers to requests for retrieval of current or future event related Geolocation information. The response may occur sometime after the request was sent. Examples include geofencing, device availability/presence alerts, sensors/beacons, alarms, etc. Relative geolocation data (distance to a specific spot), time intervals, number of occurrences and other kinds of event associated operational information can be included from this mode request.

### 4.3.2 Notification Geolocation supported operations

**HTTP GET.** Returns the list representation of all the service resources for this account, including the aforementioned properties.

**HTTP POST.** Sends a new location request and returns the representation of the Location request resource, including the aforementioned properties.

**HTTP PUT.** Updates an Immediate Geolocation request and returns the representation of the Geolocation request resource, including the aforementioned properties.

**HTTP DELETE.** Stops an Immediate Geolocation request previously created or updated.

### 4.3.3 Notification Geolocation list of required parameters

PARAMETER	DESCRIPTION
DeviceIdentifier	The target E.164 phone number or device identity of this Geolocation service.
EventGeofenceLatitude	<p>This parameter refers to the geographic coordinates' latitude of a specific location. Used to notify when a device is within a certain distance (in metres) from that specific location. WGS84 is used, whose formats for Latitude are described next. Latitude valid formats include:</p> <p>N43°38'19.39"  43°38'19.39"N  43 38 19.39  43.63871944444445</p> <p>If expressed in decimal form, northern latitudes are positive, southern latitudes are negative. The following latitude variants are also allowed:</p> <p>N43 38 19.39  43 38 19.39N</p>
EventGeofenceLongitude	<p>Same as previous, but for geographic coordinates' longitude.</p> <p>WGS84 is used, whose formats for Longitude are described next. Longitude valid formats include:</p> <p>W116°14'28.86"  116°14'28.86"W  -116 14 28.86  -116.2413513485235</p> <p>If expressed in decimal form, eastern longitudes are positive, western longitudes are negative. The following longitude variants are also allowed:</p>

	W116 14 28.86 116 14 28.86W
GeofenceRange	Distance in meters from the specific location denoted by 'EventGeofenceLatitude' and 'EventGeofenceLongitude' geographic coordinates, that would require a Geolocation procedure (e.g. as an alert that certain device is within a specific location area framed with beacons, sensors, etc.).
GeofenceEvent	Indication if this Notification Geolocation service is intended to inform about a target device entering or leaving a certain location area (implicitly specified by 'EventGeofenceLatitude', 'EventGeofenceLongitude' and 'GeofenceRange' parameters). Allowed values are: <ul style="list-style-type: none"> <li>• <b>in</b>: reports when the target device has been detected within the specified location area.</li> <li>• <b>out</b>: reports when the target device has been detected leaving the specified location area.</li> <li>• <b>in-out</b>: reports when the target device has been detected either entering or leaving the specified location area.</li> </ul>
StatusCallback	A URL that RestComm will use when the Geolocation service reaches a state that demands notifying the requesting application.

#### 4.3.4 Notification type of Geolocation examples

##### 4.3.4.1 Geolocation of a specific IP device when it enters a 1km range of a specific Geolocation - Partial and Successful answers, whole Status Callback cycle example

A curl example for a Geolocation request of a device under WiFi access whenever its distance to a specific geographic position is 1000 metres (e.g.: the

position of a beacon sensing tracking anklets of an offender). The example response provides location information every time the target device enters such location area.

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0.1:8080/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification-d
"DeviceIdentifier=56790122158" -d "EventGeofenceLatitude=-33.426280" -d
"EventGeofenceLongitude=-70.566560" -d "GeofenceRange=1000" -d "GeofenceEvent=in"
-d "StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response is displayed next for a partially-successful positioning procedure, where only last known stored location information is obtained.

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50275</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:36:15 -0500</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>56790122158</DeviceIdentifier>
    <GeolocationType>notification</GeolocationType>
    <ResponseStatus>partially-successful</ResponseStatus>
    <GeolocationData>
      <LocationTimestamp>Mon, 25 Jan 2016 16:36:15 -0500</LocationTimestamp>
      <DeviceLatitude>-34.800182</DeviceLatitude>
      <DeviceLongitude>-71.579001</DeviceLongitude>
      <Radius>178956.60</Radius>
      <InternetAddress>200.1.122.4</InternetAddress>
      <PhysicalAddress>00-50-56-C0-00-08</PhysicalAddress>
    </GeolocationData>
    <GeolocationPositioningType>last-known</GeolocationPositioningType>
    <LastGeolocationResponse>>false</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104354440b09213d04752f50275</Uri>
  </Geolocation>
</RestcommResponse>
```

Next, the corresponding status callback after a network measurement updated the previously stored last known location data is displayed (still a partially-successful positioning procedure though, desired accuracy is not accomplished yet).

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50275</Sid>
```

```

<DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
<DateUpdated>Mon, 25 Jan 2016 16:36:44 -0500</DateUpdated>
<DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
<AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
<DeviceIdentifier>56790122158</DeviceIdentifier>
<GeolocationType>notification</GeolocationType>
<ResponseStatus>partially-successful</ResponseStatus>
<GeolocationData>
  <LocationTimestamp>Mon, 25 Jan 2016 16:36:44 -0500</LocationTimestamp>
  <DeviceLatitude>-33.428423</DeviceLatitude>
  <DeviceLongitude>-70.5678026</DeviceLongitude>
  <Accuracy>220</Accuracy>
  <Radius>264.73</Radius>
  <PhysicalAddress>00-50-56-C0-00-08</PhysicalAddress>
  <InternetAddress>201.2.108.42</InternetAddress>
</GeolocationData>
<GeolocationPositioningType>Network</GeolocationPositioningType>
<LastGeolocationResponse>>false</LastGeolocationResponse>
<ApiVersion>2012-04-24</ApiVersion>
<Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104
354440b09213d04752f50275</Uri>
</Geolocation>
</RestcommResponse>

```

Finally, the corresponding response for the successful positioning procedure informed in a posterior status callback when high accuracy is accomplished through GPS assistance is shown next.

```

<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50275</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:37:04 -0500</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>56790122158</DeviceIdentifier>
    <GeolocationType>notification</GeolocationType>
    <ResponseStatus>partially-successful</ResponseStatus>
    <GeolocationData>
      <LocationTimestamp>Mon, 25 Jan 2016 16:37:04 -0500</LocationTimestamp>
      <DeviceLatitude>-33.426391</DeviceLatitude>
      <DeviceLongitude>-70.566399</DeviceLongitude>
      <Accuracy>10</Accuracy>
      <Radius>19.38</Radius>
      <PhysicalAddress>00-50-56-C0-00-08</PhysicalAddress>
      <InternetAddress>201.2.108.42</InternetAddress>
    </GeolocationData>
    <GeolocationPositioningType>GPS</GeolocationPositioningType>
    <LastGeolocationResponse>true</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>

```



```
<Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104
354440b09213d04752f50275</Uri>
</Geolocation>
</RestcommResponse>
```

#### 4.3.4.2 Geolocation of a specific IP device when it enters a 1km range of a specific Geolocation: Unauthorized Answer

A curl the exact same example of the latter Geolocation request but for an unauthorized device at the AP management system is shown below.

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification -d
"DeviceIdentifier=56790122158" -d "EventGeofenceLatitude=-33.426280" -d
"EventGeofenceLongitude=-70.566560" -d "GeofenceRange=1000" -d "GeofenceEvent=in"
-d "StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response is portrayed below.

```
<RestcommResponse>
<Geolocation>
<Sid>GLfa51b104354440b09213d04752f50276</Sid>
<DateCreated>Mon, 25 Jan 2016 16:36:10 -0500</DateCreated>
<DateUpdated>Mon, 25 Jan 2016 16:36:12 -0500</DateUpdated>
<DateExecuted>Mon, 25 Jan 2016 16:36:10 -0500</DateExecuted>
<AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
<DeviceIdentifier>56790122158</DeviceIdentifier>
<GeolocationType>notification</GeolocationType>
<ResponseStatus>unauthorized</ResponseStatus>
</GeolocationData>
<Cause>Target device not allowed by the network</Cause>
<ApiVersion>2012-04-24</ApiVersion>
<Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104
354440b09213d04752f50276</Uri>
</Geolocation>
</RestcommResponse>
```

Records are persisted when «ResponseStatus» equals «unauthorized».

#### 4.3.4.3 Geolocation of a specific IP device when it enters a 1km range of a specific Geolocation: Rejected Answer

A curl of the exact same example of the latter geolocation request but inappropriately set as «GeofenceEvent» parameter is missing.

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification -d
"DeviceIdentifier=56790122158" -d "EventGeofenceLatitude=-33.426280" -d
"EventGeofenceLongitude=-70.566560" -d "GeofenceRange=1000" -d
"GeofenceEvent=both" -d
"StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

This request gets an HTTP/1.1 400 Bad Request response with the following text.

```
StatusCallback value cannot be null
```

No records are persisted for HTTP/1.1 400 Bad Request responses, thus they cannot be updated by either a further POST or PUT request, or retrieved through a GET request.

#### 4.3.4.4 Geolocation of a specific IP device when it enters a 200 metres range of a specific Geolocation: Success Answer

A curl example for a geolocation request of a mobile phone under cellular radio access is entering or leaving a location area specified by a 200 metres distance to the geographic location of a specific business shop (e.g.: for mobile advertising) is displayed below. The example response additionally provides location information in terms of the radio access network identifiers which triggered the positioning method.

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification -d
"DeviceIdentifier=SB7089A" -d "EventGeofenceLatitude=35.526280" -d
"EventGeofenceLongitude=139.566560" -d "GeofenceRange=200" -d "GeofenceEvent=in-
out" -d
"StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response is shown below.

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50278</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 +0900</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:41:10 +0900</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 +0900</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>SB7089A</DeviceIdentifier>
    <GeolocationType>notification</GeolocationType>
    <ResponseStatus>successful</ResponseStatus>
    <GeolocationData>
      <CellId>47501A</CellId>
      <LocationAreaCode>239</LocationAreaCode>
      <MobileCountryCode>441</MobileCountryCode>
      <MobileNetworkCode>98</MobileNetworkCode>
      <NetworkEntityAddress>810002304</NetworkEntityAddress>
      <LocationAge>0</LocationAge>
      <DeviceLatitude>35.526375</DeviceLatitude>
      <DeviceLongitude>139.566802</DeviceLongitude>
      <Accuracy>50</Accuracy>
      <Radius>24</Radius>
      <LocationTimestamp>Mon, 25 Jan 2016 16:41:10 +0900</LocationTimestamp>
    </GeolocationData>
    <GeolocationPositioningType>Network</GeolocationPositioningType>
    <LastGeolocationResponse>true</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104354440b09213d04752f50278</Uri>
  </Geolocation>
</RestcommResponse>
```

#### 4.3.4.5 Geolocation of a specific IP device when it enters a 300m range of a specific Geolocation with High Accuracy: Success Answer

A curl example for a Geolocation request originated from location client within a mobile (iOS or Android) application, that expects to be informed about entering a specific location area, within 300 metres from a specific geographic spot is displayed below. The service could serve several purposes (emergency services, friends and family finder, etc.). In this case, the location information is assumed to be retrieved from an LTE-Advanced cellular network, where all location data parameters can be obtained, including parameters such as civic address («FormattedAddress» parameter).

```
curl -X POST -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification -d
"Source=59897018375" -d "DeviceIdentifier=59897018375" -d "EventGeofenceLatitude=-
34.541078" -d "EventGeofenceLongitude=-56.061600" -d "GeofenceRange=300" -d
"GeofenceEvent=in" -d "DesiredAccuracy=High" -d
"StatusCallback=http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"
```

The corresponding response is depicted next.

```
<RestcommResponse>
  <Geolocation>
    <Sid>GLfa51b104354440b09213d04752f50279</Sid>
    <DateCreated>Mon, 25 Jan 2016 16:36:10 -0300</DateCreated>
    <DateUpdated>Mon, 25 Jan 2016 16:37:18 -0300</DateUpdated>
    <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0300</DateExecuted>
    <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
    <DeviceIdentifier>59897018375</DeviceIdentifier>
    <GeolocationType>notification</GeolocationType>
    <ResponseStatus>successful</ResponseStatus>
    <GeolocationData>
      <CellId>90183B</CellId>
      <LocationAreaCode>751</LocationAreaCode>
      <MobileCountryCode>748</MobileCountryCode>
      <MobileNetworkCode>01</MobileNetworkCode>
      <NetworkEntityAddress>59800023041</NetworkEntityAddress>
      <LocationAge>0</LocationAge>
      <DeviceLatitude>-34.542029</DeviceLatitude>
      <DeviceLongitude>56.058181</DeviceLongitude>
      <Accuracy>5</Accuracy>
      <Radius>115.24</Radius>
      <PhysicalAddress>00-50-56-C0-00-08</PhysicalAddress>
      <InternetAddress>167.57.122.14</InternetAddress>
      <FormattedAddress>Avenida Italia 2643, 11500, Montevideo,
Uruguay</FormattedAddress>
      <LocationTimestamp>Mon, 25 Jan 2016 16:37:17 -0300</LocationTimestamp>
    </GeolocationData>
    <GeolocationPositioningType>GPS</GeolocationPositioningType>
    <LastGeolocationResponse>true</LastGeolocationResponse>
    <ApiVersion>2012-04-24</ApiVersion>
    <Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104
354440b09213d04752f50279</Uri>
  </Geolocation>
</RestcommResponse>
```

#### 4.3.4.6 Update previous Geolocation request for a specific IP device when it exits a 300m range of a specific Geolocation: Success Answer

Following is displayed a curl example for updating the previous geolocation request example, where geographic coordinates of the geofence location are modified, as well as the event type (leaving the location area instead of entering it as set in the previous example).

```
curl -X PUT -H "application/json"
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104
354440b09213d04752f50280 -d "EventGeofenceLatitude=-34.553098" -d
"EventGeofenceLongitude=56.050811" -d "GeofenceEvent=out"
```

The corresponding response is shown next.

```
<RestcommResponse>
<Geolocation>
  <Sid>GLfa51b104354440b09213d04752f50280</Sid>
  <DateCreated>Mon, 25 Jan 2016 16:38:10 -0300</DateCreated>
  <DateUpdated>Mon, 25 Jan 2016 16:39:18 -0300</DateUpdated>
  <DateExecuted>Mon, 25 Jan 2016 16:36:10 -0300</DateExecuted>
  <AccountSid>ACae6e420f425248d6a26948c17a9e2acf</AccountSid>
  <DeviceIdentifier>59897018375</DeviceIdentifier>
  <GeolocationType>notification</GeolocationType>
  <ResponseStatus>partially-successful</ResponseStatus>
  <GeolocationData>
    <CellId>90182A</CellId>
    <LocationAreaCode>751</LocationAreaCode>
    <MobileCountryCode>748</MobileCountryCode>
    <MobileNetworkCode>01</MobileNetworkCode>
    <NetworkEntityAddress>59800023041</NetworkEntityAddress>
    <LocationAge>0</LocationAge>
    <DeviceLatitude>-34.560071</DeviceLatitude>
    <DeviceLongitude>56.057710</DeviceLongitude>
    <Accuracy>180</Accuracy>
    <Radius>115</Radius>
    <InternetAddress>167.57.122.14</InternetAddress>
    <PhysicalAddress>00-50-56-C0-00-08</PhysicalAddress>
    <FormattedAddress>Avenida Italia 2552, 11500, Montevideo,
Uruguay</FormattedAddress>
    <LocationTimestamp>Mon, 25 Jan 2016 16:37:18 -0300</LocationTimestamp>
  </GeolocationData>
  <GeolocationPositioningType>Network</GeolocationPositioningType>
  <LastGeolocationResponse>>true</LastGeolocationResponse>
  <ApiVersion>2012-04-24</ApiVersion>
```

```
<Uri>/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104
354440b09213d04752f50280</Uri>
</Geolocation>
</RestcommResponse>
```

#### 4.3.4.7 Retrieve information of a specific previously satisfactory created Geolocation Request

Following a curl example for retrieving the information of the geolocation service request from previous example.

```
curl -X GET
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0
.1:8080/restcomm/2012-04-
24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104
354440b09213d04752f50280
```

The corresponding JSON response is displayed below (the XML response would be exactly as shown previously for the POST request).

```
{
  "sid": "GLfa51b104354440b09213d04752f50280",
  "date_created": "Mon, 25 Jan 2016 16:38:10 -0300",
  "date_updated": "Mon, 25 Jan 2016 16:39:18 -0300",
  "date_executed": "Mon, 25 Jan 2016 16:36:10 -0300",
  "account_sid": "ACae6e420f425248d6a26948c17a9e2acf",
  "device_identfier": "59897018375",
  "geolocation_type": "Notification",
  "response_status": "partially-successful",
  "geolocation_data": {
    "cell_id": "90182A",
    "location_area_code": "751",
    "mobile_country_code": 748,
    "mobile_network_code": "01",
    "network_entity_address": 59800023041,
    "location_age": 0,
    "device_latitude": "-34.560071",
    "device_longitude": "56.057710",
    "accuracy": 180,
    "internet_address": "167.57.122.14",
    "physical_address": "00-50-56-C0-00-08",
    "formatted_address": "Avenida Italia 2552, 11500, Montevideo, Uruguay",
    "location_timestamp": "Mon, 25 Jan 2016 16:37:18 -0300",
    "event_geofence_latitude": "-34.551098",
    "event_geofence_longitude": "-70.601700",
    "radius": 115
  },
}
```

```
"geolocation_positioning_type": "last-known",
"last_geolocation_response": "true",
"api_version": "2012-04-24",
"uri": "/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104354440b09213d04752f50280.json"
}
```

#### 4.3.4.8 Stop Notifications of a specific previously created Geolocation Request

Following, a curl example for stopping notifications of a previously created geolocation request.

```
curl -X DELETE
http://ACae6e420f425248d6a26948c17a9e2acf:77f8c12cc7b8f8423e5c38b035249166@127.0.0.1:8080/restcomm/2012-04-24/Accounts/ACae6e420f425248d6a26948c17a9e2acf/Geolocation/Notification/GLfa51b104354440b09213d04752f50280
```

## 4.4 Cellular Geolocation Signal Flows

Throughout this section, signal flows diagrams will be displayed between geolocation service ends, with RestComm Geolocation API and RestComm GMLC as intermediaries between the requesting application and the target device.

Figure 4.3 shows the interaction between RestComm and GMLC within a GSM network, from where location services are reduced to retrieving Global Cell Identity, Age of Location information and MSC/VLR address at which the target MSISDN is currently attached to via a MAP ATI request (subscriber's state can be included in the response if requested in MAP ATI, from which «assumed idle», «CAMEL busy» or «not provided by VLR» are the available responses).

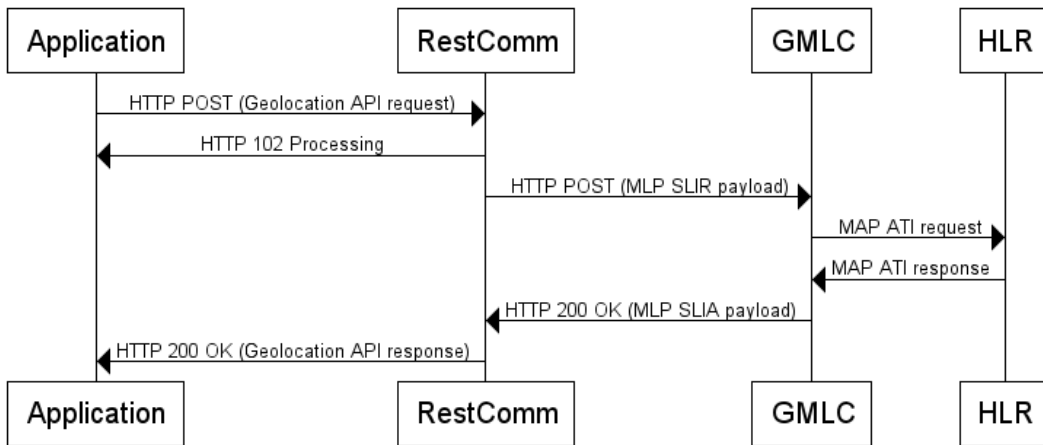


Figure 4.3. Immediate Geolocation Sequence Diagram of RestComm and GMLC in GSM Networks.

Figure 4.4 shows a Notification type of Geolocation signal flow in UMTS/3G cellular networks. An Immediate type of Geolocation signal flow in the same environment would be identical, except for the event detection and its derived signals. Besides, for the sake of simplicity, Figure 4.4 only shows a single event detection.

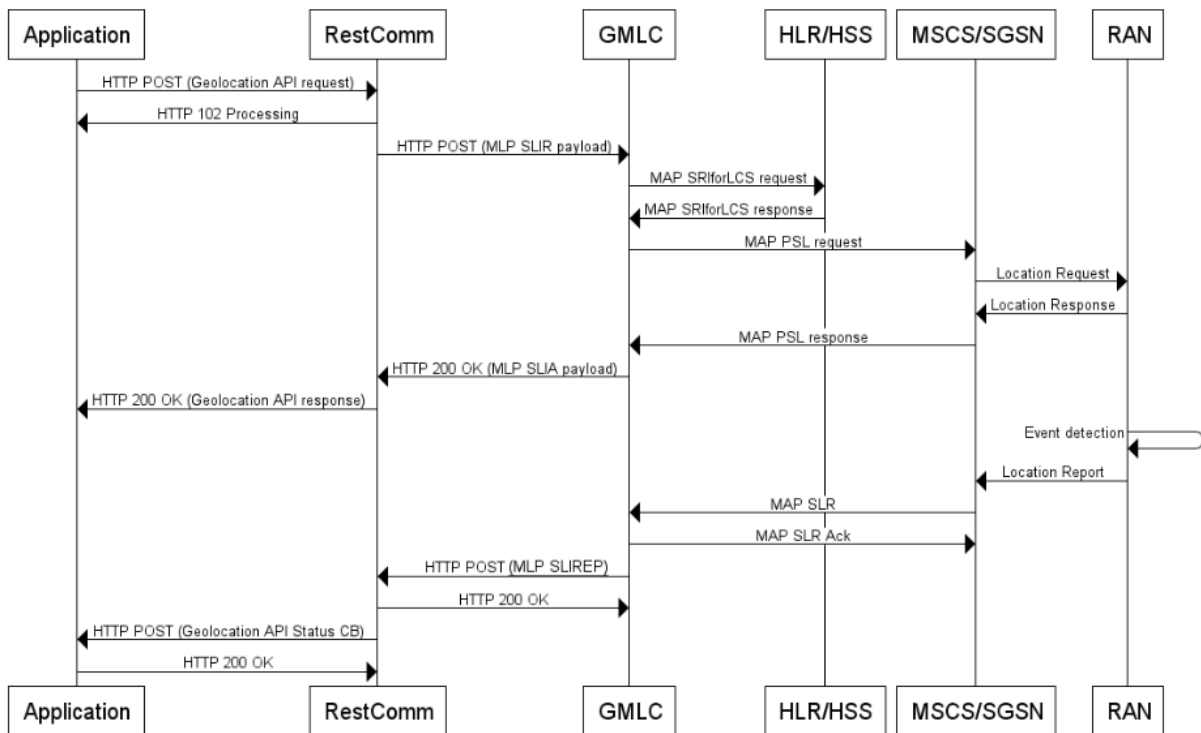


Figure 4.4. Notification type of Geolocation in UMTS/3G cellular networks.



Figure 4.5 is the analogue of Figure 4.4, but for EPS networks or LTE location services (where SS7/MAP operations do not apply anymore, but their analogous Diameter-based procedures with EPC and E-UTRAN entities).

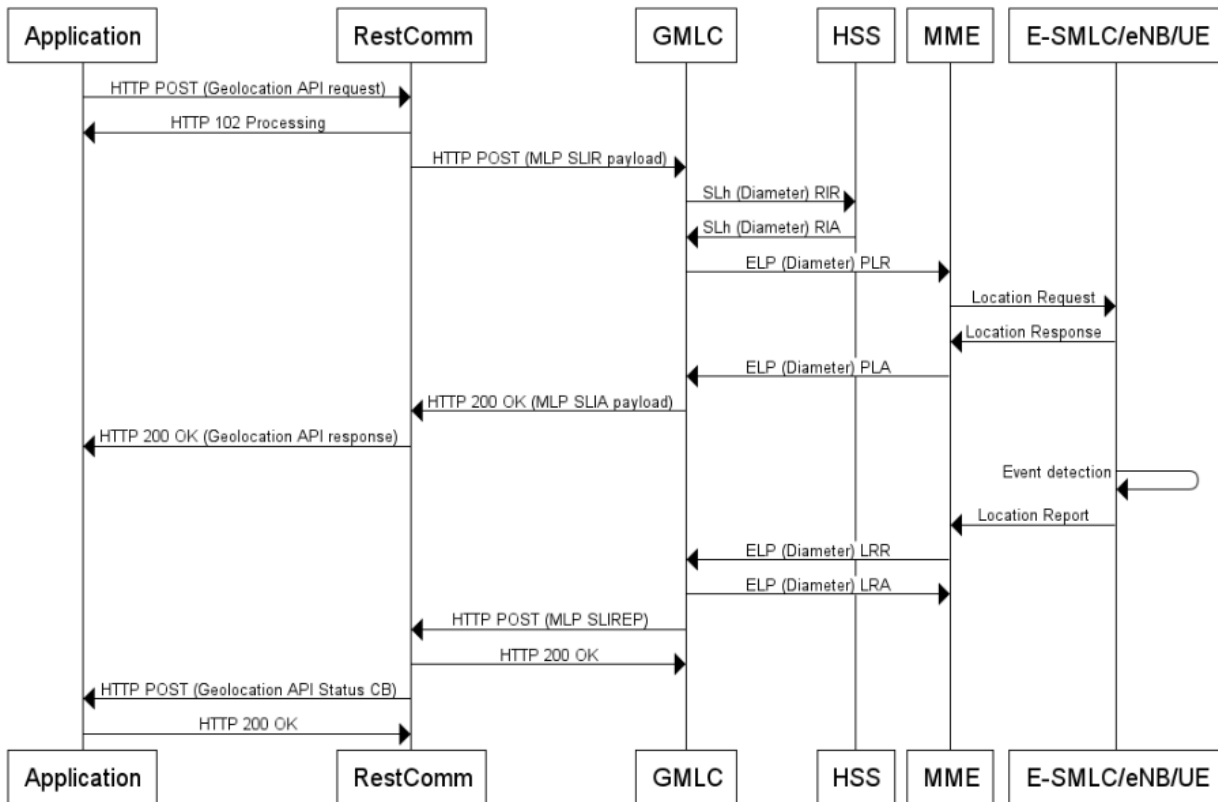


Figure 4.5. Notification type of Geolocation in 4G/LTE cellular networks.

## 4.5 IP Geolocation Signal Flow

Figure 4.5 shows an Immediate type of Geolocation signal flow in WiFi networks through RestComm iOS/Android SDK Olympus clients.

For the Notification type of Geolocation case the diagram is similar, except that the device can store the information and notify RestComm when an event is triggered, like approaching a specific location area.

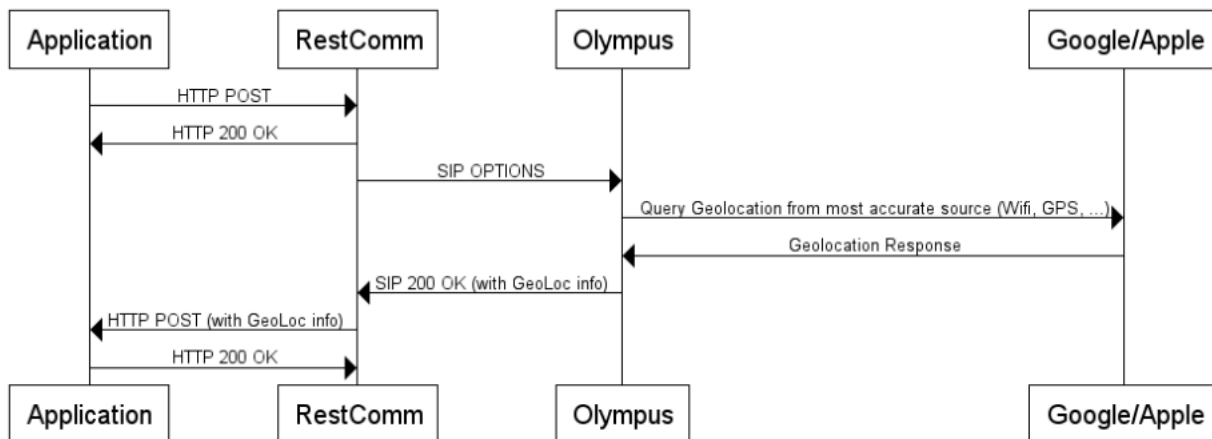


Figure 4.6. Immediate IP Geolocation sequence diagram of RestComm with Olympus clients and RestComm Mobile/Web SDKs.

## 4.6 Geolocation Status Callbacks Sequence Diagram

A Geolocation sequence diagram of RestComm API interacting with Location Servers for most accurate location information retrieved to the Status Callback URL when available.

The sequence shown reveals the best-case scenario, where status call-backs are performed until the most accurate positioning method available. As portrayed, last known stored location information is initially returned. Afterwards, a better procedure returns a more accurate location information based on the current access point. Ultimately, the best possible available method (GPS) gathers the location information and is delivered to the requesting application.

Accordingly, «LastGeolocationResponse» parameter is set to "true" in the last status call-back, as the desired accuracy is ultimately achieved.

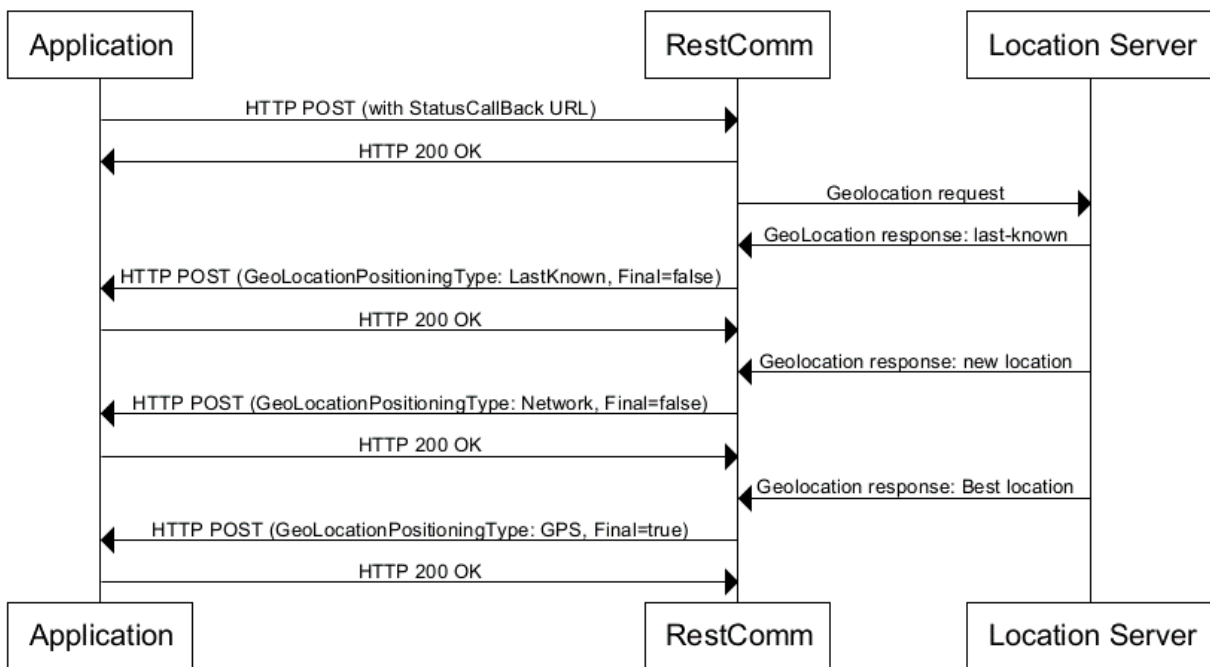


Figure 4.7. Geolocation Status Callbacks Sequence Diagram.

## 4.7 RestComm Cellular Geolocation Configuration

RestComm needs to be configured to being able to process geolocation services. The GMLC (Gateway Mobile Location Center), to whom RestComm must send the location request within cellular networks, must be configured in *restcomm.xml* file. IP address and port configuration are mandatory. Username and password are optional for GMLC.

```

<!-- TelScale GMLC -->
<gmlc>
  <gmlc-uri>GMLC_IP:PORT_NUMBER</ gmlc -uri>
  <gmlc-user></gmlc-user>
  <gmlc-password></ gmlc-password>
</gmlc>
  
```

## 4.8 RestComm RCML

The RestComm Markup Language (RCML) is composed of a set of XML tags whose purpose is instructing RestComm on how to handle a particular service, such as an on-going telephone call, a USSD session, an SMS or, beyond this project, a Geolocation service. The tags that composes the RCML are named as verbs and nouns. The combination between these elements form the path followed by RestComm during the ongoing service.

Whenever RestComm receives a call, an SMS, a USSD Pull/Push or, beyond this project, a Geolocation service, it will look up the application URL associated with the client and make a request to that URL. The response must be a valid RCML application that RestComm will execute and interact with the session. The response MIME Type should be either «text/xml» or «application/xml» and the root element of the RCML document must always be <Response> for the parser to understand.

### 4.8.1 RCML verb Geolocation

The verb <Geolocation> sends a Geolocation request either to a mobile cellular network or to an IP Geolocation application. The request could be triggered for example by an external client or during a voice call, USSD request or after reception of an SMS.

#### 4.8.1.1 Geolocation verb attributes

PARAMETER	ALLOWED VALUES	DEFAULT VALUE
deviceIdentifier	Phone number	Further described here.
action	Relative or absolute URL	None
method	GET, POST	POST
statusCallback	Relative or absolute URL	None

Table 4.3. Geolocation RCML verb attributes.

The <Geolocation> verb supports the attributes displayed in Table 4.3 and further described next:

- **deviceIdentifier.** The «deviceIdentifier» attribute takes a valid E.164 phone number, an IP or MAC address as a value. RestComm will send a location request to this target.
- **action.** The «action» attribute takes a URL as an argument. After processing the <Geolocation> verb, RestComm will make a GET or POST request to this URL with the form parameters «GeolocationStatus» and «GeolocationSid». Using an «action» URL, your application can receive synchronous notification that the Geolocation service was successfully queued. If you provide an «action» URL, RestComm will use the RCML received in your response to the «action» URL request to continue the current service. Any RCML verbs occurring after a <Geolocation> which specifies an «action» attribute are unreachable. If no «action» is provided, <Geolocation> will finish and RestComm will move on to the next RCML verb in the document. If there is no next verb, RestComm will end the service.
- **method.** The «method» attribute takes the values «GET» or «POST». This tells RestComm whether to request the «action» URL via HTTP GET or POST. This attribute is modelled after the HTML form 'method' attribute.
- **statusCallback.** The 'statusCallback' attribute takes an URL as an argument. When the location request is sent, or if sending fails, RestComm will make an asynchronous POST request to this URL with the parameters «GeolocationStatus» and «GeolocationSid». Note, «statusCallback» always uses HTTP POST to request the given URL.

#### 4.8.1.2 Request Parameters

PARAMETER	DESCRIPTION
GeolocationSid	Sid for the Geolocation service request.
GeolocationStatus	Status of the Geolocation service request. Either «sent» or «failed».

Table 4.4. RestComm Geolocation RCML request parameters.

### 4.8.1.3 Nesting

The <Geolocation> verb can have the following nouns nested: <Immediate> and <Event>.

**<Immediate>** noun: refers to requests for retrieval of current or last known location information (an associated timestamp will be included in the response). Geolocation information might include very accurate location data in terms of geographic coordinates, or just location identifiers like the radio base station transceiver identity of a cellular network that is currently giving service to the target device. Accuracy will depend on the available location procedures, either within a Mobile Network Operator for mobile handsets location within a cellular Radio Access Network, or a WLAN/WiFi covered area for IP location.

**<Notification>** noun: refers to requests for retrieval of event related location information. Examples include geofencing, device availability/presence alerts, sensors/beacons alarms, etc. Relative location data (distance to a specific spot), time intervals of occurrence and other kinds of event associated operational information can be included from this mode request.

The <Immediate> noun does not bring up additional attributes to the <Geolocation> verb. Contrariwise, the <Notification> noun adds additional attributes that are discussed in next section.

#### 4.8.1.3.1 Notification noun attributes

PARAMETER	ALLOWED VALUES	DEFAULT
eventGeofencingLatitude	A valid latitude universal coordinate.	Null
eventGeofencingLongitude	A valid longitude universal coordinate.	Null
geofenceRange	An integer amount to represent a distance in metres.	Null
geofenceEvent	A string representing the type of geofencing event to be notified.	Null

Table 4.5. Notification noun attributes.

The <Notification> noun adds additional attributes depicted in Table 4.5 are further discussed next.

- **eventGeofencingLatitude.** The 'eventGeofencingLatitude' attribute refers to the geographic coordinates' latitude of a specific location. Used to notify when a device is within a certain distance (in metres) from that specific location.
- **eventGeofencingLongitude.** The 'eventGeofencingLongitude' attribute refers to the geographic coordinates' longitude of a specific location. Used to notify when a device is within a certain distance (in metres) from that specific location.
- **geofenceRange.** The «geofenceRange» attribute refers to the distance in metres from a specific geographic location denoted by «eventGeofencingLatitude» and «eventGeofencingLongitude».
- **geofenceEvent.** The «geofenceEvent» attribute refers to the eventuality of a target device entering or leaving a specific location area (implicitly specified by «EventGeofenceLatitude», «EventGeofenceLongitude» and «GeofenceRange»). Available values are:
  - **in:** reports when the target device has been detected within the specified location area.
  - **out:** reports when the target device has been detected leaving the specified location area.
  - **in-out:** reports when the target device has been detected either entering or leaving the specified location area.

#### 4.8.1.4 RCML Geolocation verb examples

RCML examples on how to use the <Geolocation> verb are depicted next. Immediate Geolocation service example demanding a synchronous HTTP POST action:

```
<Response>
  <Geolocation>
    <Immediate deviceIdentifier="59899549878"
action="http://my.controller.net" method="POST"/>
  </Geolocation>
</Response>
```

Immediate Geolocation service example demanding an asynchronous HTTP POST:

```
<Response>
  <Geolocation>
    <Immediate deviceIdentifier="59899549878"
statusCallback="http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"/>
  </Geolocation>
</Response>
```

Notification Geolocation service example demanding a synchronous HTTP GET action:

```
<Response>
  <Geolocation>
    <Notification deviceIdentifier="59899549878" eventGeofencingLatitude="-
33.426280" eventGeofencingLongitude="-70.566560W" geofenceRange="500"
geofenceEvent="in-out"
action="http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf" method="GET"/>
  </Geolocation>
</Response>
```

Notification Geolocation service example demanding an asynchronous HTTP POST:

```
<Response>
  <Geolocation>
    <Notification deviceIdentifier="59899549878" eventGeofencingLatitude="-
33.426280" eventGeofencingLongitude="-70.566560W" geofenceRange="500"
```



```
geofenceEvent="in-out"  
statusCallback="http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf"/>  
  </Geolocation>  
</Response>
```

When the Geolocation request is sent, or if sending fails, RestComm will make an asynchronous POST method to the 'StatusCallback' URL with the parameters «GeolocationStatus» and «GeolocationSid», as explained in the RestComm RCML Geolocation section. Examples of this method, applicable to previous examples for either «sent» or «failed» requests, are exhibited next.

```
HTTP    POST    http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf    -d  
"GeolocationSid=GLd66d2fe3954b4c888ad3dafc81b8f661" -d "GeolocationStatus=sent"
```

```
HTTP    POST    http://192.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf    -d  
"GeolocationSid=GLd66d2fe3954b4c888ad3dafc81b8f661" -d "GeolocationStatus=failed"
```

#### 4.8.2 RestComm Visual Designer and Geolocation verb

RestComm Visual Designer (RVD) comprises a user-friendly Service Creation Environment (SCE) that allows telecommunication application development above RestComm core platform. It includes of a visual editor to rapidly create the applications and a controller, which is basically a RCML generator to be executed by RestComm Service Execution Environment (SEE).

By the time being, three types of RVD projects can be generated: Voice, SMS and USSD. RestComm interacts as an IMS SIP-AS and therefore, it dialogs via SIP/RTP with a Session Border Controller (SBC) or PSTN Gateway for voice services, or TeleStax Enterprise SMSC and USSD Gateway for either SMS or USSD respectively.

From this work onwards, the Geolocation verb can be used in RVD in whichever project is chosen. Next figures show an example of an RVD USSD project where the «Geolocation» verb is selected in one of the modules of the service call flow, whether the Geolocation type chosen is «Immediate» or «Notification». Icons and words used in RVD do not exactly match with RestComm Geolocation API and RCML definitions (the translation is part of RestComm inner JavaScript development).

The screenshot shows the Teletax RESTCOMM visual service designer interface. The top bar displays the logo and the text "RESTCOMM visual service designer" along with the user "administrator@company.com". The main workspace is titled "USSD\_LBS" and contains a "Location" module configuration. The configuration includes the following fields:

- Assign reply to:** geolocation
- Scope:** application
- MobilePhone:** Score\_From
- Source:** Score\_From
- Location Type:** Immediate
- Continue to:** SelectAction
- Method:** POST
- Status callback:** http://52.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf

Figure 4.8. Example of Geolocation verb usage in RVD USSD project (Immediate).

The screenshot shows the Teletax RESTCOMM visual service designer interface. The top bar displays the logo and the text "RESTCOMM visual service designer" along with the user "administrator@company.com". The main workspace is titled "USSD\_LBS" and contains a "Location" module configuration. The configuration includes the following fields:

- Assign reply to:** geolocation
- Scope:** application
- MobilePhone:** Score\_From
- Source:** Score\_From
- Location Type:** Notification
- Geofence event:** In
- Continue to:** SelectAction
- Method:** POST
- Status callback:** http://52.16.1.19:8080/ACae6e420f425248d6a26948c17a9e2acf
- Geofence Latitude:** 35.8902891, N/S, South
- Geofence Longitude:** 58,1903467, W/E, West
- Geofence Range:** 300, Metric, Metres

Figure 4.9 Example of Geolocation verb usage in RVD USSD project (Notification).

## Chapter 5

### 5 RestComm GMLC

#### 5.1 GMLC summary and enhancements introduced

As already stated, GMLC stands for Gateway Mobile Location Centre. Its existence enables offering LBS to mobile subscribers roaming across several Mobile Network Operator's Radio Access Networks, regardless of the type of access (GERAN, UTRAN or E-UTRAN).

Existing PLMN (Public Land Mobile Network) network elements are proprietary and run on non-standard operating environments located in trusted operator's zones which make it difficult to build and deploy new applications. Also, these network elements do not provide the tools and interfaces needed to access and retrieve data from content providers over the Internet. The GMLC connects to these network elements and enables the flow of LCS messages to be extended to an open, standards-based Application Server (AS) located in the IP network. The AS also provides the tools and interfaces to enable access to content providers through the Internet.

In one PLMN (Public Land Mobile Network), there may be more than one GMLC. A GMLC is the first node an external LCS client accesses in a PLMN.

As already stated in section 2.2, a GMLC can retrieve the modest location information known as Cell Global Identity (CGI) as for the latest MAP Update Location operation between the HLR and VLR by issuing a MAP ATI request to the HLR (Home Location register). Hence, CGI represents the location information with

greatest error margin retrievable by a GMLC in GSM based core networks. CGI through MAP ATI was until this project the only available procedure in RestComm GMLC. As for 3GPP specs, hypothetically a Stand-Alone SMLC can be placed within the BSC for triggering more precise location procedures, but in practice this is hardly found. Until this work, RestComm GMLC was endowed only with this capability.

The project subject of this project provided RestComm GMLC the corresponding extensions for achieving greater location capabilities either for GSM (in theory), UMTS/HSPA+ or LTE/LTE-Advanced. Besides, «wiring» RestComm Geolocation API to RestComm GMLC, provides even wider VAS proficiencies, beyond MNO's Core Networks protocols, offering Web developers an enabler to transparently develop LBS within cellular networks.

More accurate positioning methods were developed for cellular networks, particularly from 3G (UMTS) and beyond. Naturally, accuracy comes with a price. When these dearer location capabilities are available, the GMLC may request routing information from the HLR via the Lh interface or HSS (Home Subscriber Server) via the SL<sub>h</sub>/ L<sub>h</sub> interface.

While Lh interface reside in a Circuit-Switched Core Network and therefore demands SS7 MAP operations, SL<sub>h</sub> is placed in the Evolved Packet Core (EPC) and is a Diameter-based interface for LTE location services, as specified by [45]. After performing registration authorization, it may send positioning requests to either VMSC (Visited Mobile Switching Centre), SGSN (Serving GPRS Support Node), MSCS (Mobile Switching Centre Server) or MME (Mobility Management Entity) and receives final location estimates from the corresponding entity via the L<sub>g</sub>, L<sub>gd</sub> or SL<sub>g</sub> interface. Again, L<sub>g</sub>/ L<sub>gd</sub> interfaces demand SS7 MAP operations while SL<sub>g</sub> is a Diameter-based interface for LTE location occupying ELP procedures, where ELP stands for EPC Location Protocol as specified by [44].

Up to this point, what is known in 3GPP specifications as «Immediate Location Request» has been covered. These kinds of requests are approached in RestComm Geolocation API as «Immediate Geolocation». A GMLC can also handle «Deferred Location Request», which represents retrieving of location contingent on some current or future events where the response from the LCS Server to the LCS Client

may occur sometime after the request was sent, as described in [126]. When a deferred location request is triggered by the GMLC, event-based «Subscriber Location Reports», either conveyed through MAP or ELP are sent back to the GMLC by the entity at which the target mobile equipment is attached to (VMSC, MSCS, SGSN or MME). Figure 5.1 exhibits TeleStax Enterprise GMLC (productized version of RestComm GMLC) architecture and interfaces with aforementioned entities and RestComm (and particularly, RestComm Geolocation API).

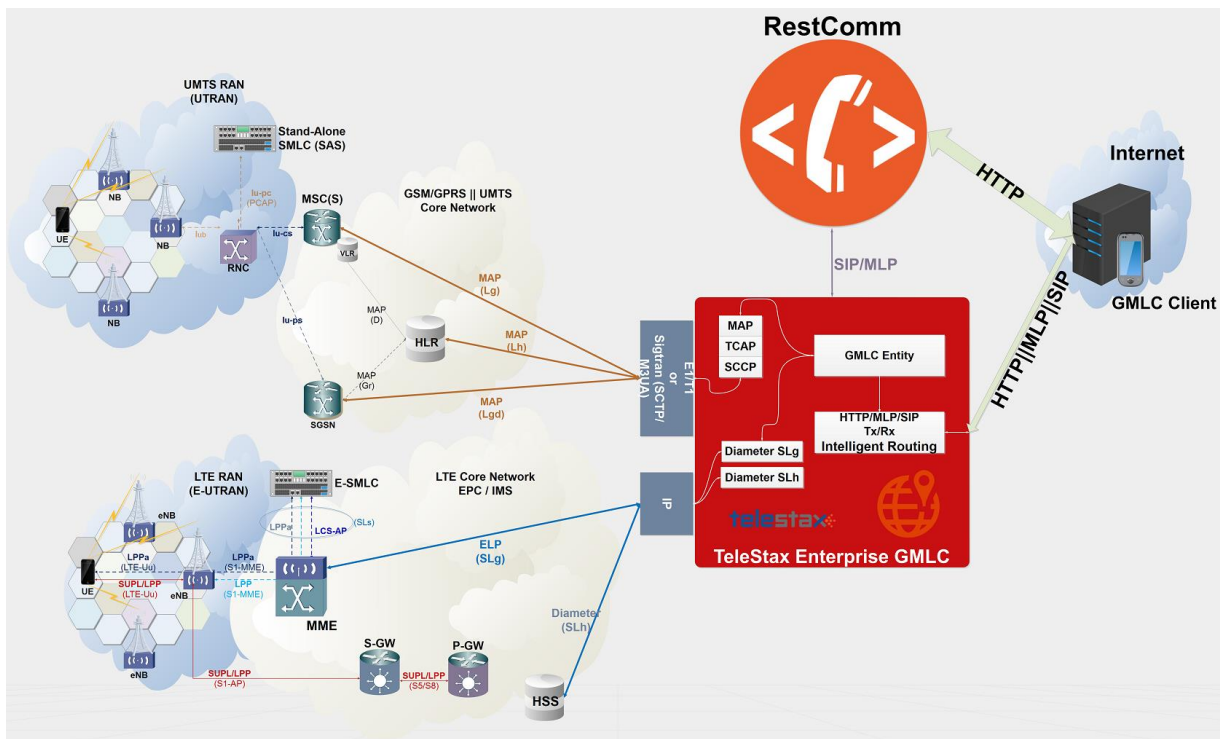


Figure 5.1. RestComm GMLC in heterogeneous networks environments.

As this work aimed to provide mechanisms for providing VAS within heterogeneous networks, regarding RestComm GMLC needed to take care of providing support for the following MAP and Diameter-based operations for LCS (Location Services) within MNO’s Circuit-Switched or Packet-Switched Core Networks:

- **MAP SRIforLCS:** Send Routing Information for Location Services, to gather IMSI and core network entity address (MSC or SGSN) to which send further location request.

- **MAP PSL:** Provide Subscriber Location, to gather location information from the UTRAN (UMTS Terrestrial Radio Access Network), which should include, besides Cell Global Identity, location estimates in geographic coordinates of the target User Equipment, depending on available positioning methods (e.g. E-OTD, OTDOA, UTDOA, A-GPS, etc.).
- **MAP SLR:** Subscriber Location Report, to gather location of a target User Equipment from the MSC or SGSN when a request for location is either implicitly administered or made at some earlier time in MAP PSL for event based deferred type of location.
- Diameter Routing Information Request/Answer (**RIR/RIA**): analogous to MAP SRIforLCS but over Diameter based SL<sub>h</sub> interface between GMLC and HSS.
- ELP Provide Location Request/Answer (**PLR/PLA**): analogous to MAP PSL but over Diameter-based Evolved Packet Core Location Protocol (ELP) SL<sub>g</sub> interface between GMLC and MME.
- ELP Location Report Request/Answer (**LRR/LRA**): analogous to MAP SLR, but over Diameter-based Evolved Packet Core Location Protocol (ELP) SL<sub>g</sub> interface between GMLC and MME.

Figure 5.2 shows the signal flow between RestComm/TeIScale GMLC and UMTS Core Network Entities in the most complex scenario, i.e. when MAP PSL request issues not only the immediate response, but a deferred location request. Hence, after an event is detected in the UTRAN, a location update is sent back to the GMLC through a MAP SLR operation. Figure 5.3 displays the same described scenario but within EPS for LTE location services. So, for the latter, SL<sub>h</sub> RIR/RIA and ELP PLR/PLA LRR/LRA Diameter based messages are exchanged between GMLC and HSS and MME respectively.

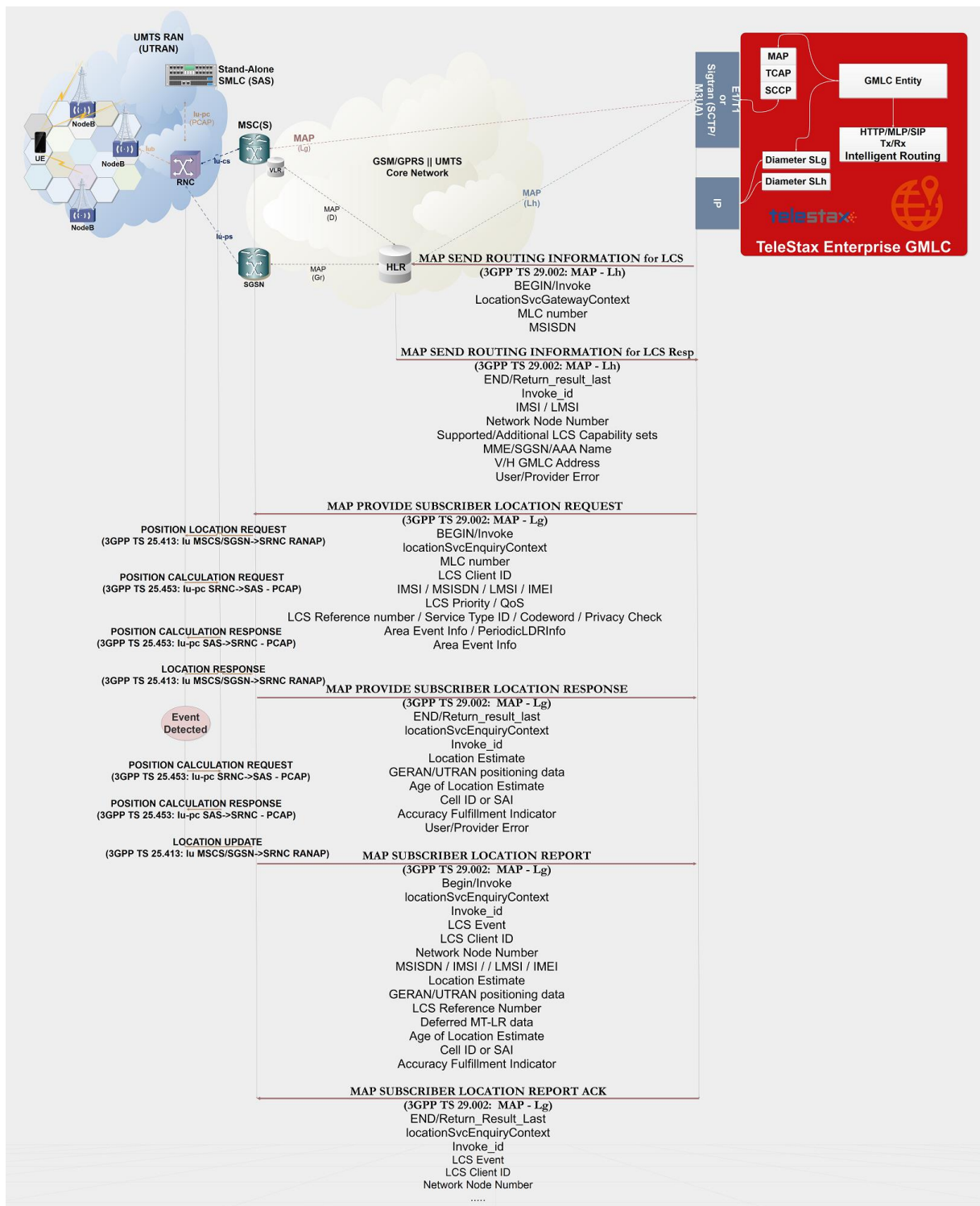


Figure 5.2. TeleStax Enterprise/RestComm GMLC LCS signal flow in UMTS.

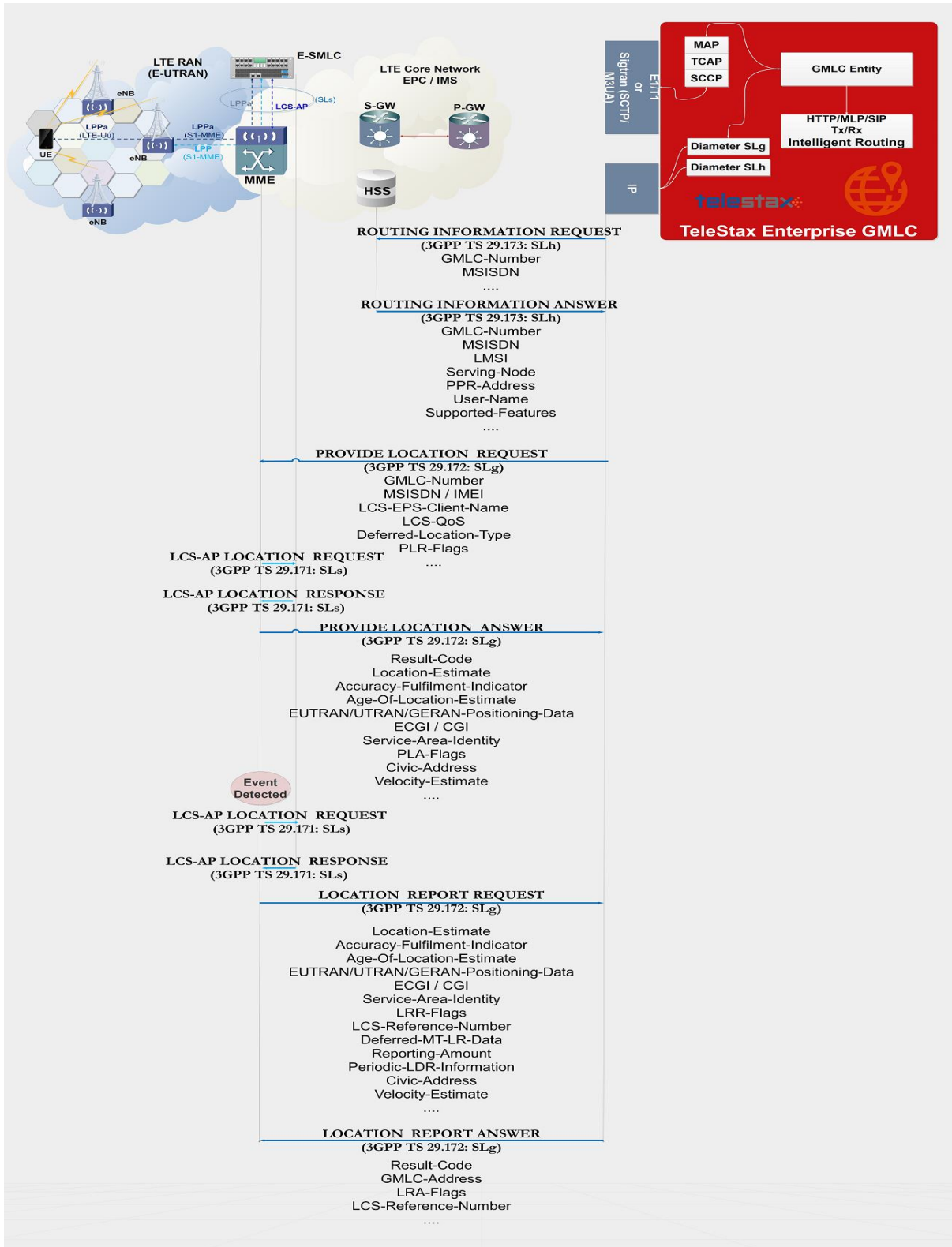


Figure 5.3. TeleStax Enterprise/RestComm GMLC LCS signal flow in LTE.



In order to make the aforementioned enhancements possible, work needed to be done to couple already developed MAP operations in jSS7 in RestComm GMLC. The final product is as shown Figure 5.4, which depicts RestComm GMLC main software functional blocks and interfaces with underlying network entities. Please also notice on top presence of RestComm Geolocation API at the API exposure layer of TeleStax' communication platform, as well as client side enablers RestComm iOS and Android SDKs. The latter shall be able to interact through RestComm Geolocation API with RestComm GMLC in the future. Also, RestComm Visual Designer is graphically displayed as an originator of location services on RestComm GMLC via RestComm Geolocation API as described earlier.

As either  $SL_h$  or  $SL_g$  interfaces were not present in jDiameter protocol stack (neither were correspondent JAIN SLEE Resource Adaptors), first they needed to be developed from scratch and then integrated to RestComm GMLC.

Next section shall describe the work done for the development of these interfaces within the RestComm jDiameter framework, which then needed to be embedded as part of the low-level protocol stacks of RestComm GMLC middleware, beyond jSS7. Therefore, a brief introduction to jDiameter shall come first. Please refer to Annex F for this, where examples of execution of  $SL_h$  or  $SL_g$  interfaces with all AVPs populated are shown. Likewise, next section in this chapter contains examples involving execution of location services within this interfaces through the work done in Restcomm jDiameter in this regard, which is public and can be reached at [130-132].

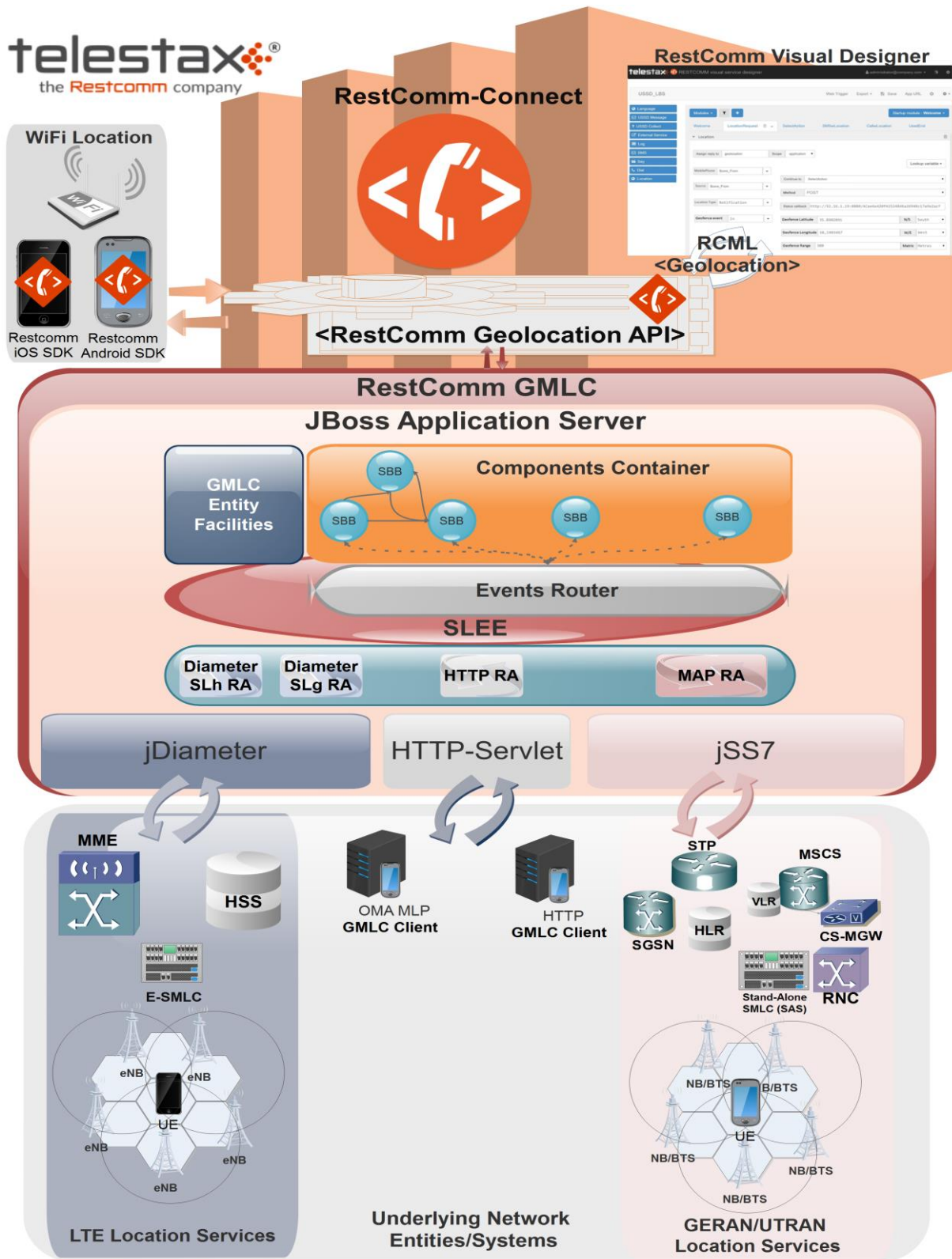


Figure 5.4. RestComm GMLC Software Architecture and Interfaces.

## 5.2 HTTP Procedures for Location Requests

TeleStax Enterprise GMLC makes use of HTTP protocol between the gateway and the third-party applications (or Value Added Service Modules). TeleStax Enterprise GMLC might receive location service requests from third-party applications and then translates these requests to SS7 MAP or Diameter based commands when applies. The HTTP call-back mechanism allows the third-party application to be agnostic to Operating System, Programming Language and Framework.

GMLC service begins when the network sends an HTTP (GET/POST) request to the GMLC. Figure 5.5 displays the signal flow between an application and TeleStax Enterprise/RestComm GMLC within an GSM Core Network, from where location services are reduced to retrieving Global Cell Identity, Age of Location information and MSC/VLR address at which the target MSISDN is currently attached to, by means of a MAP ATI request to the HLR (subscriber’s state can be included in the response if requested in MAP ATI, from which «assumedIdle», «camelBusy» or «notProvidedByVlr» are the available responses).

The application, via a REST Web Service, delivers an HTTP GET request to TeleStax Enterprise/RestComm GMLC. TeleStax Enterprise/RestComm GMLC then performs a MAP ATI request to the concerning GSM Core Network HLR and receives the corresponding response with location information as previously stated.

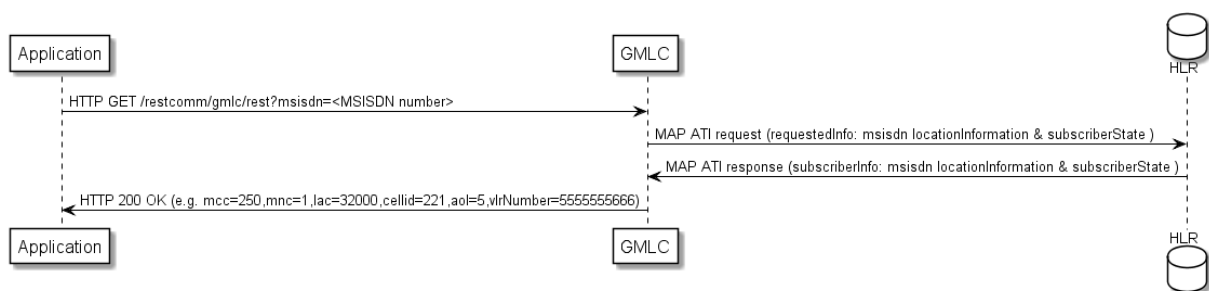


Figure 5.5. Example of simple GMLC GSM location service triggered by HTTP GET.

A deeper look inside the messages exchanged as for the previous diagram is shown next (all information depicted are example taken from Wireshark traces).

See the HTTP GET procedure next.

```

Internet Protocol Version 4, Src: 192.168.26.1, Dst: 192.168.26.128
Transmission Control Protocol, Src Port: 48200 (48200), Dst Port: 8080 (8080),
Seq: 1, Ack: 1, Len: 509
Hypertext Transfer Protocol
  GET /restcomm/gmlc/rest?msisdn=59899077937 HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /restcomm/gmlc/rest?msisdn=59899077937
HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /restcomm/gmlc/rest?msisdn=59899077937
  Request Version: HTTP/1.1

```

The triggered MAP ATI request and response Wireshark traces extracts are shown next. MAP ATI Request:

```

IP 4, Src: 192.168.26.128, Dst: 41.188.110.5
SCTP, Src Port: 8012 (8012), Dst Port: 8011 (8011)
MTP 3 User Adaptation Layer (M3UA)
SCCP
  Called Party address
    SubSystem Number: HLR (Home Location Register) (6)
    Global Title 0x4 (9 bytes)
      Called Party Digits: 59899077937
  Calling Party address
    SubSystem Number: GMLC(MAP) (145)
    Global Title 0x4 (6 bytes)
      Calling Party Digits: 222333
TCAP
  begin
    dialogueRequest
      application-context-name: 0.4.0.0.1.0.29.3 (anyTimeInfoEnquiryContext-
v3)
      components: 1 item
        Component: invoke
          invokeID: 0
          opCode: localValue: 71
GSM MAP
  Component: invoke (1)
    invoke
      invokeID: 0
      opCode: anyTimeInterrogation (71)
      subscriberIdentity: msisdn (1)
        msisdn: 919598097739f7
      requestedInfo
        locationInformation
        subscriberState
      gsmSCF-Address: 91223233

```

## MAP ATI Response:

```

IP 4, Src: 41.188.110.5, Dst: 192.168.26.128
SCTP, Src Port: 8011 (8011), Dst Port: 8012 (8012)
MTP 3 User Adaptation Layer (M3UA)
SCCP
  Called Party address
    SubSystem Number: GMLC(MAP) (145)
    Global Title 0x4 (6 bytes)
    Calling Party Digits: 222333
  Calling Party address
    SubSystem Number: HLR (Home Location Register) (6)
    Global Title 0x4 (9 bytes)
    Called Party Digits: 59899077937
TCAP
  end
  Destination Transaction ID
  oid: 0.0.17.773.1.1.1 (id-as-dialogue)
  dialogueResponse
    application-context-name: 0.4.0.0.1.0.29.3 (anyTimeInfoEnquiryContext-
v3)
    result: accepted (0)
  components: 1 item
    Component: returnResultLast
      invokeID: 0
      opCode: localValue: 71
GSM MAP
  Component: returnResultLast (2)
  returnResultLast
    invokeID: 0
    resultretres
      opCode: localValue (0)
      localValue: anyTimeInterrogation (71)
      subscriberInfo
        locationInformation
          ageOfLocationInformation: 5
          geographicalInformation: 104f01231f9a0e00
          vlr-number: 915555556566
          cellGlobalIdOrServiceAreaIdOrLAI:
cellGlobalIdOrServiceAreaIdFixedLength: 52f0107d0000dd
          subscriberState: assumedIdle (0)
          assumedIdle

```

The HTTP GET response sent from the GMLC to the requesting application is shown next.

```

IP Version 4, Src: 192.168.26.128, Dst: 192.168.26.1
Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 48200 (48200),
Seq: 230, Ack: 510, Len: 5
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n

```

```

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
[HTTP response 1/1]
[Time since request: 0.341487879 seconds]
[Request in frame: 10]
HTTP chunked response
  Data chunk (61 octets)
  End of chunked encoding
  \r\n
Data (61 bytes) mcc=250,mnc=1,lac=32000,cellid=221,aol=5,vlrNumber=5555555666

```

Figure 4.3 of previous chapter displays the analogous signal flow as the one explained before, but including RestComm Geolocation API between the application and TeleStax Enterprise GMLC. In this case, MAP ATI is triggered by RestComm by an HTTP POST request with OMA MLP «Standard Location Immediate Request» (SLIR). The terms MLP SLIR/SLIA and SLIREP stand for Mobile Location Protocol Standard Location Immediate Request/Response/Report as for OMA (Open Mobile Alliance) Mobile Location Protocol 3.1 specification [107]. The mentioned MLP SLIR example is depicted next:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE svc_init SYSTEM "MLP_SVC_INIT_310.DTD">
<svc_init xmlns="MLP_SVC_INIT_310.dtd">
  <hdr>
    <client>
      <id>ACae6e420f425248d6a26948c17a9e2acf</id>
      <pwd>f8bc1274677b173d1a1cf3b9924eaa7e</pwd>
      <serviceid>0005</serviceid>
    </client>
  </hdr>
  <slir>
    <msids>
      <msid type="MSISDN">59899077937</msid>
    </msids>
    <loc_type type="CURRENT" />
  </slir>
</svc_init>

```

The corresponding answer to the MLP SLIR request (after reception of MAP ATI response from GSM network), i.e. the MLP SLIA (Standard Location Immediate Answer) embedded in HTTP POST response is shown next.

```

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE svc_result SYSTEM
"MLP_SVC_RESULT_310.DTD">

```

```

<svc_result xmlns="MLP_SVC_RESULT_310.dtd" ver="3.1.0">
  <slia ver="3.1.0">
    <pos>
      <msid>59899077937</msid>
      <pd>
        <time utc_off="-0300">20160828181421</time>
        <plmn>
          <mcc>250</mcc>
          <mnc>1</mnc>
        </plmn>
        <gsm_net_param>
          <cgi>
            <mcc>250</mcc>
            <mnc>1</mnc>
            <lac>32000</lac>
            <cellid>221</cellid>
          </cgi>
          <neid>
            <vlrid>
              <vlrno>5555555666</vlrno>
            </vlrid>
          </neid>
        </gsm_net_param>
      </pd>
    </pos>
  </slia>
</svc_result>

```

Figure 4.5 of previous chapter displays an analogous signal flow as the one explained before including RestComm Geolocation API between the application and TeleStax Enterprise GMLC, but in this case, Diameter SL<sub>h</sub> RIR/RIA and SL<sub>g</sub> (ELP) PLR are triggered by RestComm by the HTTP POST containing OMA MLP SLIR. The mentioned MLP SLIR example would be almost identical to the one shown for GSM location, but with some differences and additions as shown next:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE svc_init SYSTEM "MLP_SVC_INIT_310.DTD">
<svc_init xmlns="MLP_SVC_INIT_310.dtd">
  <hdr>
    <client>
      <id>ACae6e420f425248d6a26948c17a9e2acf</id>
      <pwd>f8bc1274677b173d1a1cf3b9924eaa7e</pwd>
      <serviceid>0005</serviceid>
    </client>
  </hdr>
  <slir>
    <msids>
      <msid type="MSISDN">59899077937</msid>
    </msids>
  </slir>
</svc_init>

```

```

    </msids>
    <loc_type type="CURRENT" />
    <geo_info>
      <CoordinateReferenceSystem>
        <Identifier>
          <code>4326</code>
          <codeSpace>EPSG</codeSpace>
          <edition>6.1</edition>
        </Identifier>
      </CoordinateReferenceSystem>
    </geo_info>
    <change_area>
      <target_area>
        <name_area>a51</name_area>
      </target_area>
      <type>MS_WITHIN_AREA</type>
      <loc_estimates>FALSE</loc_estimates>
      <no_of_reports>1</no_of_reports>
    </change_area>
    <duration>3600</duration>
    <lcs_ref>579</lcs_ref>
  </slir>
</svc_init>

```

Corresponding transmission of ELP PLR to the LTE network is shown next (only AVPs shown for simplicity):

```

[PLR] Sending Request: 8388620 [E2E:1263534084 -- HBH:1693441831 --
AppID:16777255]
[PLR] Request AVPs:
[PLR] <avp name="Session-Id" code="263" vendor="0" value="51.0.0.1;343;
3840918879;SLg-PLA34277987203" />
[PLR] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
[PLR]   <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
[PLR]   <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
[PLR] </avp>
[PLR] <avp name="Destination-Realm" code="283" vendor="0" value="tel1.com" />
[PLR] <avp name="Origin-Realm" code="296" vendor="0" value="restcomm.com" />
[PLR] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
[PLR] <avp name="Origin-Host" code="264" vendor="0" value="aaa://51.0.0.1:13868"
/>
[PLR] <avp name="SLg-Location-Type" code="2500" vendor="10415" value="0" />
[PLR] <avp name="MSISDN" code="701" vendor="10415" value="59899077937" />
[PLR] <avp name="LCS-EPS-Client-Name" code="2501" vendor="10415">
[PLR]   <avp name="LCS-Name-String" code="1238" vendor="10415" value="
ACae6e420f425248d6a26948c17a9e2acf" />
[PLR]   <avp name="LCS-Format-Indicator" code="1237" vendor="10415" value="2" />
[PLR] </avp>
[PLR] <avp name="LCS-Client-Type" code="1241" vendor="10415" value="1" />
[PLR] <avp name="LCS-Requestor-Name" code="2502" vendor="10415">
[PLR]   <avp name="LCS-Requestor-Id-String" code="1240" vendor="10415"
value="Restcomm Geolocation API" />

```



```
[PLR] <avp name="LCS-Format-Indicator" code="1237" vendor="10415" value="0" />
[PLR] </avp>
[PLR] <avp name="LCS-Priority" code="2503" vendor="10415" value="1" />
[PLR] <avp name="LCS-QoS" code="2504" vendor="10415">
[PLR] <avp name="LCS-QoS-Class" code="2523" vendor="10415" value="1" />
[PLR] <avp name="Horizontal-Accuracy" code="2505" vendor="10415" value="120" />
[PLR] <avp name="Vertical-Accuracy" code="2506" vendor="10415" value="99999" />
[PLR] <avp name="Vertical-Requested" code="2507" vendor="10415" value="0" />
[PLR] <avp name="Response-Time" code="2509" vendor="10415" value="1" />
[PLR] </avp>
[PLR] <avp name="Deferred-Location-Type" code="2532" vendor="10415" value="4" />
[PLR] <avp name="LCS-Reference-Number" code="2531" vendor="10415" value="579" />
[PLR] <avp name="Area-Event-Info" code="2533" vendor="10415">
[PLR] <avp name="Occurrence-Info" code="2538" vendor="10415" value="0" />
[PLR] <avp name="Interval-Time" code="2539" vendor="10415" value="3600" />
[PLR] </avp>
[PLR] <avp name="Area-Definition" code="2534" vendor="10415">
[PLR] <avp name="Area-Type" code="2536" vendor="10415" value="2" />
[PLR] <avp name="Area-Identification" code="2537" vendor="10415" value="a51" />
[PLR] </avp>
[PLR] <avp name="PLR-Flags" code="2545" vendor="10415" value="4" />
[PLR] <avp name="Area-Event-Info" code="2533" vendor="10415">
[PLR] <avp name="Reporting-Amount" code="2541" vendor="10415" value="1" />
[PLR] <avp name="Reporting-Interval" code="2542" vendor="10415" value="3600" />
[PLR] </avp>
[PLR] </avp>
[PLR] <avp name="GMLC-Address" code="2405" vendor="10415" value="52.21.78.91" />
[PLR] <avp name="PLR-Flags" code="2545" vendor="10415" value="4" />
[PLR] </avp>
```

Reception of ELP PLA from the LTE network is shown next (only AVPs shown for simplicity):

```
[PLA] Received Answer: 8388620 [E2E:1263534084 -- HBH:1693441831 --
AppID:16777255]
[PLA] Request AVPs:
[PLA] <avp name="Session-Id" code="263" vendor="0" value="51.0.0.1;343;
3840918879;SLg-PLA34277987203" />
[PLA] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
[PLA] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
[PLA] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
[PLA] </avp>
[PLA] <avp name="Result-Code" code="268" vendor="0" value="2001" />
[PLA] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
[PLA] <avp name="Location-Estimate" code="1242" vendor="10415"
value="S35°38'15.37" W58°45'21.77" />
[PLA] <avp name="Accuracy-Fulfilment-Indicator" code="2513" vendor="10415"
value="0" />
[PLA] <avp name="Age-Of-Location-Estimate" code="2514" vendor="10415" value="0" />
[PLA] <avp name="EUTRAN-Positioning-Data" code="2516" vendor="10415"
value="0A73F937" />
[PLA] <avp name="ECGI" code="2517" vendor="10415" value="EFB9437" />
```

```

[PLA] <avp name="Serving-Node" code="2401" vendor="10415">
[PLA]   <avp name="SGSN-Number" code="1489" vendor="10415" value="59899004501" />
[PLA]   <avp name="SGSN-Name" code="2409" vendor="10415" value="SGSN01" />
[PLA]   <avp name="SGSN-Realm" code="2410" vendor="10415" value="sgsn.tel1.com" />
[PLA]   <avp name="MME-Name" code="2402" vendor="10415" value="MME710" />
[PLA]   <avp name="MME-Realm" code="2408" vendor="10415" value="mme.tel1.com" />
[PLA]   <avp name="3GPP-AAA-Server-Name" code="318" vendor="10415"
value="aaa.restcomm.com" />
[PLA]   <avp name="LCS-Capabilities-Sets" code="2404" vendor="10415"
value="99900123" />
  [PLA]   <avp name="GMLC-Address" code="2405" vendor="10415" value="52.21.78.91"
/>
[PLA] </avp>
[PLA] <avp name="PLA-Flags" code="2546" vendor="10415" value="0" />
[PLA] <avp name="ESMLC-Cell-Info" code="2552" vendor="10415">
[PLA]   <avp name="ECGI" code="2517" vendor="10415" value="EFB9437" />
[PLA]   <avp name="Cell-Portion-ID" code="2553" vendor="10415" value="0" />
[PLA] </avp>

```

The corresponding answer to the MLP SLIR request (after reception of ELP PLA from the LTE network), i.e. the MLP SLIA (Standard Location Immediate Answer) embedded in HTTP POST response is shown next.

```

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE svc_result SYSTEM
"MLP_SVC_RESULT_310.DTD">
<svc_result xmlns="MLP_SVC_RESULT_310.dtd" ver="3.1.0">
  <slia ver="3.1.0">
    <req_id>579</req_id>
    <pos>
      <msid>59899077937</msid>
      <pd>
        <time utc_off="-0300">20161023235151</time>
        <geo_info>
          <CoordinateReferenceSystem>
            <Identifier>
              <code>4326</code>
              <codeSpace>EPSG</codeSpace>
              <edition>6.1</edition>
            </Identifier>
          </CoordinateReferenceSystem>
          <shape>
            <CircularArea>
              <coord>
                <X>35 38 15.375</X>
                <Y>58 45 21.77W</Y>
              </coord>
              <radius>-1</radius>
            </CircularArea>
          </shape>
        </geo_info>
      </pd>
    </pos>
  </slia>
</svc_result>

```

```

        </geo_info>
    </pd>
</pos>
</slia>
</svc_result>

```

When the settled event occurs, it triggers a location report back to the GMLC, the ELP LRR/LRA messages are subsequently conveyed back and forth between the MME and GMLC, as displayed next:

```

[LRR] Sending Request: 8388621 [E2E:1370488836 -- HBH:1693543583 --
AppID:16777255]
[LRR] Request AVPs:
[LRR] <avp name="Session-Id" code="263" vendor="0" value="51.0.0.1;343;
3841024432;-SLg-LRR34277987203" />
[LRR] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
[LRR]   <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
[LRR]   <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
[LRR] </avp>
[LRR] <avp name="Destination-Realm" code="283" vendor="0" value="restcomm.com" />
[LRR] <avp name="Origin-Realm" code="296" vendor="0" value="tel1.com" />
[LRR] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
[LRR] <avp name="Origin-Host" code="264" vendor="0" value="aaa://51.0.0.1:13868"
/>
[LRR] <avp name="Location-Event" code="2518" vendor="10415" value="4" />
[LRR] <avp name="LCS-EPS-Client-Name" code="2501" vendor="10415">
[LRR]   <avp name="LCS-Name-String" code="1238" vendor="10415"
value="ACae6e420f425248d6a26948c17a9e2acf" />
[LRR]   <avp name="LCS-Format-Indicator" code="1237" vendor="10415" value="2" />
[LRR] </avp>
[LRR] <avp name="3GPP-IMSI" code="1" vendor="10415" value="748039876543210" />
[LRR] <avp name="MSISDN" code="701" vendor="10415" value="59899077937" />
[LRR] <avp name="IMEI" code="1402" vendor="10415" value="011714004661057" />
[LRR] <avp name="Location-Estimate" code="1242" vendor="10415" value="
S35°37'10.91" W58°01'33.07"" />
[LRR] <avp name="Accuracy-Fulfilment-Indicator" code="2513" vendor="10415"
value="0" />
[LRR] <avp name="Age-Of-Location-Estimate" code="2514" vendor="10415" value="3" />
[LRR] <avp name="Velocity-Estimate" code="2515" vendor="10415" value="0" />
[LRR] <avp name="EUTRAN-Positioning-Data" code="2516" vendor="10415"
value="0A73F937" />
[LRR] <avp name="ECGI" code="2517" vendor="10415" value="E1F0023" />
[LRR] <avp name="Service-Area-Identity" code="1607" vendor="10415" value="service-
area-umts-3" />
[LRR] <avp name="LCS-Service-Type-ID" code="2520" vendor="10415" value="234" />
[LRR] <avp name="Pseudonym-Indicator" code="2519" vendor="10415" value="0" />
[LRR] <avp name="LCS-QoS-Class" code="2523" vendor="10415" value="1" />
[LRR] <avp name="Serving-Node" code="2401" vendor="10415">
[LRR]   <avp name="SGSN-Number" code="1489" vendor="10415" value="59899004501" />
[LRR]   <avp name="SGSN-Name" code="2409" vendor="10415" value="SGSN01" />
[LRR]   <avp name="SGSN-Realm" code="2410" vendor="10415" value="sgsn.tel1.com" />

```

```

[LRR] <avp name="MME-Name" code="2402" vendor="10415" value="MME710" />
[LRR] <avp name="MME-Realm" code="2408" vendor="10415" value="mme.tel1.com" />
[LRR] <avp name="3GPP-AAA-Server-Name" code="318" vendor="10415"
value="aaa.restcomm.com" />
[LRR] <avp name="LCS-Capabilities-Sets" code="2404" vendor="10415"
value="99900123" />
[PLA] <avp name="GMLC-Address" code="2405" vendor="10415" value="52.21.78.91"
/>
[LRR] </avp>
[LRR] <avp name="LRR-Flags" code="2530" vendor="10415" value="0" />
[LRR] <avp name="LCS-Reference-Number" code="2531" vendor="10415" value="579" />
[LRR] <avp name="Deferred-MT-LR-Data" code="2547" vendor="10415">
[LRR] <avp name="Deferred-Location-Type" code="2532" vendor="10415" value="4" />
[LRR] <avp name="Termination-Cause" code="2548" vendor="10415" value="7" />
[LRR] </avp>
[LRR] <avp name="GMLC-Address" code="2405" vendor="10415" value="52.21.78.91" />
[LRR] <avp name="Periodic-LDR-Info" code="2540" vendor="10415">
[LRR] <avp name="Reporting-Amount" code="2541" vendor="10415" value="8639910" />
[LRR] <avp name="Reporting-Interval" code="2542" vendor="10415" value="8639998"
/>
[LRR] </avp>
[LRR] <avp name="ESMLC-Cell-Info" code="2552" vendor="10415">
[LRR] <avp name="ECGI" code="2517" vendor="10415" value="EFC9452" />
[LRR] <avp name="Cell-Portion-ID" code="2553" vendor="10415" value="12393" />
[LRR] </avp>
[LRR] <avp name="1xRTT-RCID" code="2554" vendor="10415" value="00000010" />
[LRR] <avp name="Civic-Address" code="2556" vendor="10415" value="<civicAddress
xml:lang='en-GB' xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
xmlns:cdc="http://devon.canals.example.com/civic">
  <country>UY</country>
  <A1>MV</A1>
  <ap:airport>MVD</ap:airport>
  <ap:terminal>Carrasco International</ap:terminal>
  <ap:concourse>A</ap:concourse>
  <ap:gate>4</ap:gate>
</civicAddress>" />
[LRR] <avp name="Barometric-Pressure" code="2557" vendor="10415" value="101327" />

```

```

[LRA] Received Answer: 8388621 [E2E:1370488836 -- HBH:1693543583 --
AppID:16777255]
[LRA] Request AVPs:
[LRA] <avp name="Session-Id" code="263" vendor="0" value="51.0.0.1;343;
3841024432;-SLg-LRR34277987203" />
[LRA] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
[LRA] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
[LRA] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
[LRA] </avp>
[LRA] <avp name="Result-Code" code="268" vendor="0" value="2001" />
[LRA] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
[LRA] <avp name="GMLC-Address" code="2405" vendor="10415" value="52.21.78.91" />
[LRA] <avp name="LRA-Flags" code="2549" vendor="10415" value="0" />
[LRA] <avp name="Reporting-PLMN-List" code="2543" vendor="10415">

```

```
[LRA] <avp name="Visited-PLMN-Id" code="1407" vendor="10415" value="74803,
74801" />
[LRA] <avp name="Periodic-Location-Support-Indicator" code="2550" vendor="10415"
value="1" />
[LRA] <avp name="Prioritized-List-Indicator" code="2551" vendor="10415"
value="0" />
[LRA] </avp>
[LRA] <avp name="PLMN-ID-List" code="2544" vendor="10415">
[LRA] <avp name="Visited-PLMN-Id" code="1407" vendor="10415" value="74803,
74801" />
[LRA] <avp name="Periodic-Location-Support-Indicator" code="2550" vendor="10415"
value="1" />
[LRA] </avp>
[LRA] <avp name="LCS-Reference-Number" code="2531" vendor="10415" value="579" />
[LRR] <avp name="Origin-Host" code="264" vendor="0" value="51.0.0.1" />
[LRR] <avp name="Origin-Realm" code="296" vendor="0" value="restcomm.com" />
```

The corresponding answer MLP SLIREP (Standard Location Immediate Report) embedded in HTTP POST response is shown next.

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE svc_result SYSTEM
"MLP_SVC_RESULT_310.DTD">
<svc_result xmlns="MLP_SVC_RESULT_310.dtd" ver="3.1.0">
  <slirep ver="3.1.0">
    <lcs_ref>579</lcs_ref>
    <pos>
      <msid>59899077937</msid>
      <imsi>748039876543210</imsi>
      <imei>011714004661057</imei>
      <speed>0</speed>
      <pd>
        <time utc_off="-0300">20161023235901</time>
        <geo_info>
          <CoordinateReferenceSystem>
            <Identifier>
              <code>4326</code>
              <codeSpace>EPSG</codeSpace>
              <edition>6.1</edition>
            </Identifier>
          </CoordinateReferenceSystem>
          <shape>
            <CircularArea>
              <coord>
                <X>35 37 10.91S</X>
                <Y>58 01 33.07W</Y>
              </coord>
              <radius>100</radius>
            </CircularArea>
          </shape>
        </geo_info>
      </pd>
    </pos>
```

```
</slirep>  
</svc_result>
```

Then, as explained up to this point, TeleStax Enterprise GMLC (or its public version, RestComm GMLC) comprises a complete solution in heterogeneous networks including the following highlights:

- User Equipment location in either GSM BSS, UMTS UTRAN or LTE E-UTRAN via SS7 MAP or Diameter based SL<sub>h</sub> and SL<sub>g</sub> interfaces procedures.
- REST interface with third party applications via HTTP POST/GET with carrier grade performance compliance.
- OMA MLP [107] compliance for GMLC clients.
- Interworking with TeleStax RestComm Geolocation API.

As for any TeleStax Enterprise platform, GMLC needed to pass through performance tests for its release. The following figures show successful performance test statistics for tests carried out during 93 minutes at 90000 samples per minute (HTTP POST/GET commands translated to MAP/Diameter messages). HTTP stats show «five nines rule compliance», i.e. 99.999% success rate for carrier grade performance (less than 0.001% error count, i.e. 721 out of 1.831.575 HTTP samples, or mean of 1 error throughout 10.000 HTTP samples bursts, on 10% CPU and no more than 2.5 GB of RAM average usage).

ci.telestax.com/view/Telscale-SS7/job/Telscale-gmlc-Performance-GetLoc/113/artifact/results/PerfCorderAnalysis.html

Test Duration(seconds)= 5610

Java

Meas	Stats	Graph
GcMemBefore	category=Java count=176.0 geometricMean=2558.3251095738487 kurtosis=40.03281838034191 max=2797.0 mean=2570.0 median=2590.5 min=753.0 percentile25=2507.25 percentile5=2266.8 percentile75=2684.25 percentile95=2776.3 quadraticMean=2577.5821695746367 skewness=-4.782750014432591 stdDev=198.1233670505036 sum=452320.0 sumSquares=1.169331652E9 variance=39252.868571428575	<p><b>GcMemBefore</b> CollFreq:4</p>
Cpu	category=Java count=1121.0 geometricMean=9.05606865145411 kurtosis=334.4734333657053 max=20.71 mean=9.06520963425513 median=9.01 min=8.23 percentile25=8.86 percentile5=8.64 percentile75=9.14 percentile95=9.76 quadraticMean=9.077402690609981 skewness=13.80102353863272 stdDev=0.4705437353818442 sum=10162.0999999999975 sumSquares=92369.54760000002 variance=344783.96461386513	<p><b>Cpu</b> CollFreq:4</p>
GcMemAfter	category=Java count=176.0 geometricMean=572.1750738948042 kurtosis=-0.8621186461882244 max=762.0 mean=579.4090909090909 median=565.5 min=371.0 percentile25=506.5 percentile5=442.7 percentile75=653.5 percentile95=744.45 quadraticMean=586.6856154395098 skewness=0.30577699211925546 stdDev=92.37750330509651 sum=101976.0 sumSquares=6.0579202E7 variance=8533.603116883116	<p><b>GcMemAfter</b> CollFreq:4</p>
GcPauseDuration	category=Java count=176.0 geometricMean=121.74881702525029 kurtosis=170.1473313685453 max=760.0 mean=124.28977272727272 median=122.0 min=92.0 percentile25=120.0 percentile5=105.85 percentile75=124.0 percentile95=127.0 quadraticMean=133.40154268564172 skewness=12.931222565131563 stdDev=48.59466293981022 sum=21875.0 sumSquares=3132091.0 variance=2361.441266233765	<p><b>GcPauseDuration</b> CollFreq:4</p>

Figure 5.6. GMLC performance test: CPU and memory consumption statistics [129].

ci.telestax.com/view/TelScale-SS7/job/TelScale-gmlc-Performance-GetLoc/113/artifact/results/PerfCorderAnalysis.html

HTTP		
Meas	Stats	Graph
HTTPElapsed	category=HTTP count=721.0 geometricMean=144.09847781152908 kurtosis=7.360474383028285 max=10058.0 mean=917.6047156726762 median=86.0 min=64.0 percentile25=79.0 percentile5=74.0 percentile75=158.5 percentile95=10022.0 quadraticMean=2870.2001126309056 skewness=3.0553379004116055 stdDev=2721.455964068981 sum=661593.0 sumSquares=5.939633103E9 variance=7406322.564366627	
HTTPErrorCount	category=HTTP count=721.0 geometricMean=0.0 kurtosis=10.567524655371434 max=2.0 mean=0.08460471567267686 median=0.0 min=0.0 percentile25=0.0 percentile5=0.0 percentile75=0.0 percentile95=1.0 quadraticMean=0.3002541687982387 skewness=3.335187592368598 stdDev=0.2882878392431921 sum=61.0 sumSquares=65.0 variance=0.0831098782555086	
HTTPSampleCount	category=HTTP count=721.0 geometricMean=2539.790661159302 kurtosis=3.673618177516437 max=2638.0 mean=2540.3259361997225 median=2550.0 min=2242.0 percentile25=2515.5 percentile5=2444.0 percentile75=2577.0 percentile95=2603.0 quadraticMean=2540.8503018847987 skewness=-1.4309661775030973 stdDev=51.653605943194464 sum=1831575.0 sumSquares=4.654718505E9 variance=2668.0950069348146	

Figure 5.7. GMLC performance test: HTTP samples statistics [129].



## Chapter 6

# 6 Evaluation

## 6.1 Evaluation method analysis

Given the nature of this work, enormous challenges were faced to make an evaluation as the following would be needed:

- An MNO's infrastructure containing all needed components, i.e. all core and radio access networks elements either for legacy or NGN's. At the present moment, very few MNOs comply with all these needed components.
- A relationship with such kind of exceptional MNO and its will to carry out the tests. This would require a commercial bound between the latter and TeleStax (or one of its partners). Not an impossible task at all (in fact, we are in initial conversations with some of them), but it would demand too much time only in paperwork for acquiring executive permission for the task.
- A simulation environment compatible with TeleStax Open Source frameworks containing all elements needed. At the moment, although it's planned to carry out a «dangerous demo» for TADSummit [133] (most probably during 2017 event), such simulation environment does not exist.

Therefore, DESMET [100] methodologies became as a feasible evaluation option. DESMET is intended to help a particular organisation to plan and execute an unbiased and reliable evaluation of software engineering methods/tools. The DESMET evaluation methodology separates evaluation exercises into two main categories:

- **Quantitative** evaluations: Identification of the benefits in quantifiable terms or measurable effects that a new method/tool is expected to provide to an organisation.
- **Qualitative** evaluations: they are aimed at establishing method/tool appropriateness, i.e. how well a new method/tool fits the needs and culture of an organisation and its relationship to the features or functionality to be implemented to introduce a paradigm shift. Evaluators analyse the extent to which the new method/tool meets the expected functionality based on personal experience.

The term organisation is meant to apply to a software development group in a particular company/division performing broadly similar tasks under similar conditions, or academic institutions interested in experimental software engineering.

DESMET defines three ways of organizing an evaluation exercise:

- **Formal Experiment:** investigation where many subjects (i.e. software engineers) are asked to perform one or several tasks (or variety of tasks) using the different methods/tools under investigation. Subjects are assigned to each method/tool such that results are unbiased and can be analysed using standard statistical techniques;
- **Case Study:** investigation where each method/tool under investigation is tried out on a real project using the standard project development procedures of the evaluating organisation;
- **Survey:** where staff/organisations that have used specific methods or tools on past projects are asked to provide information about the method or tool. Information from the method/tool users can be analysed using standard statistical techniques. It applies to subjects with experience in the usage of similar methods/tools.

By combining the latter evaluation ways and categories, nine evaluation methods emerge:

- ✓ Quantitative experiment.
- ✓ Quantitative case study.
- ✓ Quantitative survey.
- ✓ Qualitative screening.

- ✓ Qualitative experiment.
- ✓ Qualitative case study.
- ✓ Qualitative survey.
- ✓ Hybrid method 1 (Qualitative effects analysis).
- ✓ Hybrid method 2 (Benchmarking).

These nine evaluation options are further divided in three categories: quantitative, qualitative and hybrid evaluation methods. As for the specific case of this work, given the context described at the beginning of this chapter, it must be stated that its evaluation will not be focused on quantitative values (although we already have some like the ones shown in figures 5.6 and 5.7 for GMLC performance tests), but it will be emphasized on the analysis of the capabilities and innovative characteristics of the implementation comprising this work. Given this scenario, the three quantitative evaluation methods are discarded. From the pending six ones, qualitative screening is discarded as there's not available literature describing the software method/tools rather than actual use of the methods/tools for initial screening. Qualitative case study is discarded as for the time being it is not possible to make a test of the whole system in the real-life scenario it is thought for, as briefly explained earlier in this chapter. Within this same context/cause, qualitative experiment, qualitative effects analysis and benchmarking are also discarded. Then, only one possible evaluation method is available: **qualitative survey**. As for DESMET, a qualitative survey consists of a feature-based evaluation done by experts or people who have had experience of using the method/tool, or have studied the method/tool. The difference between a survey and an experiment is that participation in a survey is at the discretion of the subject.

So, a qualitative survey is entirely feasible, even though the number of competent subjects for the task is not vast, as they not only need to be proficient in several subjects around mobile telecommunication networks, location based services and signaling protocols, but also familiar with the software environment/framework used, as well as the software versioning system used: Git [140], as well as the public repository: GitHub [141]. Having previously followed TeleStax Open Source Playbook [122] guidelines would be a plus. Very few people match all these credentials. Then, we selected:

- Andrew Eross, CTO of Locatrix [E3] and contributor to the GMLC project on MLP;

- Jean Deruelle, CTO of TeleStax;
- James Body, Head of Research and Development at Truphone [E4];
- Marcelo Aranibar, Core Network Planning and Optimization Manager at Tigo Bolivia;
- Julio Rey, lead developer of American Prepaid VAS [E5], founded by Osmar Coronel (CEO), former Millicom Regional CTO (1990 to 2013).

On related notes, Andrew Eross and Julio Rey participated in TADHack Uruguay (organized by the author of this work, sponsored by TeleStax, Locatrix and University ORT Uruguay, besides TADHack organization). Their demo and speech around their «JAL» hack, is included in the event's blog [E22]; James Body, along with Mark White (CEO of Locatrix) was one of the enthusiast «brainstormers» after the presentation of this project at Restconn 2015 as can be witnessed in [E16].

## 6.2 Qualitative Surveys

The subjects conducting the qualitative survey were provided with an evaluation guide where they need to provide their name and date of the evaluation, as well as answering a questionnaire. Evaluation comprises two aspects, documentation assessment and software testing. Then, in first place evaluators are asked to assess RestComm Geolocation API and RCML documentation [E6-E7] and RestComm GMLC Admin Guide [E8] (which includes description for LTE location services as for [44-45], as described in chapter 5, implemented in jDiameter for this work). Following, evaluators are asked to conduct a software test simulation, consisting in performing HTTP queries to Restcomm Geolocation API (as the ones described in sections 4.2.4 and 4.3.4, also exposed in [E6]) and corresponding tests in RestComm GMLC. For the latter, chapter 3 in RestComm GMLC Admin Guide [E8] provides all the needed steps to run the Gateway and conduct these tests in simulator mode. Special binaries extracted from local Git repositories were provided to the evaluators (as some of the work done is for the time being, under peer review or Beta testing -hence, this evaluation exercise is very rich in terms of Quality Assurance for TeleStax too as a software vendor-). After having conducted both phases of the evaluation, they are asked to fill a questionnaire in the following format.

Evaluation Question				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

Evaluation questions are listed next.

#### Part 1: documentation assessment

- 1) RestComm Geolocation API design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.
- 2) RestComm Geolocation RCML design, definition and documentation is fully comprehensible and effectively applies for RestComm Visual Designer implementation of Location Based Services.
- 3) RestComm Geolocation API effectively provides a user-friendly tool for easily building Location Based Services.
- 4) RestComm Geolocation API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.

#### Part 2: software testing

- 5) RestComm Geolocation API provides adequate means for Web developers to request location information (i.e. cURL).
- 6) RestComm Geolocation API provides appropriate format for Web developers to gather location information (i.e. XML or JSON).
- 7) RestComm Geolocation API effectively gathers a comprehensive set of immediate or event driven location information.
- 8) RestComm Geolocation API effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications.

- 9) RestComm GMLC effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.
- 10) RestComm GMLC effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures.
- 11) RestComm GMLC effectively provides Carrier Grade performance as for [E9].
- 12) RestComm GMLC effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed).
- 13) RestComm jDiameter implementation of SLh and SLg interfaces for LTE location services as for 3GPP TS 29.172/29.173 [44-45] effectively complies with the needs of gathering location services from an LTE network being them embedded in RestComm GMLC, and the former complies with 3GPP/LTE specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed).
- 14) RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.

The survey provides sufficient information around the general objective of this work, i.e. «enabling Value-Added Services deployment within heterogeneous networks environments, by developing transparent messaging and positioning mechanisms according to international standardization organizations, with focus on 3GPP/LTE technical specifications». Furthermore, the research question is both implicitly and explicitly formulated, i.e. «How to provide Location Based Services (LBS) triggered by asynchronous messaging events according to 3GPP/LTE specifications so as to making them work universally and transparently regardless of user equipment and radio access network».

Table 6.1 shows the results of the evaluation survey and Annex G the individual answers. As it can be seen, all evaluators qualified as being in complete agreement for most of the questions placed in the questionnaire. Please refer to that annex for further details and valuable comments.

Question	Score					Acceptation
	Fully disagree	Disagree	Neutral	Agree	Fully agree	
<b>PART 1. Documentation assessment</b>						
1					5	100%
2					5	100%
3				1	4	95%
4					5	100%
<b>PART 2. Software testing</b>						
5					5	100%
6					5	100%
7					5	100%
8					5	100%
9					5	100%
10					5	100%
11				2	3	90%
12					5	100%
13					5	100%
14					5	100%

Table 6.1. Summary of the evaluation survey results.





## Chapter 7

# 7 Conclusions and Future Work

## 7.1 Results

As a result of the activities carried out, the following products have been accomplished, available to the entire telecommunication software development community, given the open source nature of the chosen framework.

**RestComm Geolocation API:** first Open Source API [E6] for interaction with mobile networks and retrieval of location information under cellular radio access networks and/or WiFi. The design and framework chosen for the API's development allow adding value to new or pre-existing telecommunication services across heterogeneous networks. In other words, gathered mobile location information might be retrieved autonomously or triggered by asynchronous events from messaging services, voice, etc., independently of the underlying network infrastructure. According to the final evaluation, the following aspects of the «RestComm Geolocation API» are highlighted:

- API's design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.
- RestComm Markup Language design, definition and documentation is fully comprehensible and effectively applies for a Service Creation Environment (SCE) like RestComm Visual Designer, for the implementation of Location Based Services.
- The API effectively provides a user-friendly tool for easily building Location Based Services.

- The API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.
- The API effectively provides adequate means for Web developers to request (i.e. cURL) and gather location information (i.e. XML or JSON).
- The API effectively effectively gathers a comprehensive set of immediate or event driven location information.
- The API effectively effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications.

Release of the first Open Source **Gateway Mobile Location Centre** [E8] according to international standardization groups such as 3GPP/LTE and OMA for the retrieval of location information under any radio access network. According to the final evaluation, the following aspects of the «**RestComm GMLC**» are highlighted:

- Effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.
- Effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures.
- Effectively provides Carrier Grade performance.
- Effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed).
- Effectively complies with the needs of gathering location services from an LTE network being RestComm jDiameter implementation of SL<sub>h</sub> and SL<sub>g</sub> interfaces embedded in RestComm GMLC, and the former complies with 3GPP/LTE specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed).

Only Open Source development of Diameter based **SL<sub>h</sub> y SL<sub>g</sub> interfaces** [130-132] for **LTE location services** according to 3GPP TS 29.172/29.173 [44-45].

**RestComm Geolocation API** and **RestComm GMLC** comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind

of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.

## 7.2 Future work

This section will describe next steps already outlined as part of TeleStax roadmap concerning Geolocation services:

- Implement security mechanisms for Geolocation requests (e.g. HTTPS, black lists of MSISDNs/requestors, etc.).
- Geolocation history tracking mechanisms for further VAS.
- Global Cell Identity / Service Area Identity → latitude/longitude conversion database.
- RestComm iOS / Android SDKs integration RestComm Geolocation API.
- RestComm iOS / Android SDKs integration of USSI and Instant Messaging (SMS) for triggering location services via RestComm-Connect, either over WiFi/GPS assisted applications, or through RestComm GMLC.
- Enhancement of RestComm Visual Designer with RestComm RCML Geolocation verb for voice, SMS and USSD projects, along with stand-alone Geolocation projects.
- Expand implementation of already implemented OMA MLP requests/answers.
- Development of SL<sub>s</sub> Diameter based interface between MME and E-SMLC according to 3GPP TS 29.171 guidelines [43].

- Development from scratch of a Stand-Alone SMLC and E-SMLC for providing the full stack to Mobile Network Operators which most of them do not yet own.
- User plane location via SUPL. This will make RestComm GMLC a Gateway for either the control and user plane, therefore, location clients might perceive it either as a GMLC or a SLP (SUPL Location Platform). Still to decide whether integrating it in a single unified module, or two communicated instances working independently in either planes, such as MSCS and CS-MGW accomplish together for routing and connecting voice calls in the UMTS.
- Integration of work done by IIT R&D group for dispatchable location in indoors environments via WiFi [139] and Bluetooth (the latter being currently under investigation by some members of this group).
- Web trigger location via voice RestComm Visual Designer projects. Through this method, any browser with WebRTC capabilities would be enabled to obtain geographic coordinates from a target device (e.g. a CRM agent could get location information when receiving a call from a customer).

This roadmap will be available for the Open Source community, which might include academic endeavours. Some of them have already been set as issues in RestComm projects at [github.com/RestComm](https://github.com/RestComm) projects. Other endeavours involve ongoing business full solutions, like the aforementioned commented MFS platform for Africa and Latin American countries. Every line of code that will be committed for this project will be available in already newly opened project under RestComm brand (i.e. <https://github.com/RestComm/restcomm-mfs>).

Finally, another very important topic to address here is TeleStax sponsoring of TADHack events [E21]. Last TADHack of 2016 was carried out during October, so RestComm Geolocation API will make its debut during first TADHack in 2017. For every student willing to participate in the future work of this project, TADHack might be the point of entrance. Many developers of TeleStax core team were recruited after winning a TADHack event, and following TeleStax Open Source R&D playbook [122]. So, hopefully many contributions related to this work will come from the Open Source community and further academic endeavours like the one that motivated this work.

## Bibliography

- [1] "ITU-T Recommendations and other publications," *ITU*. [Online]. Available: <http://www.itu.int/en/ITU-T/publications/Pages/default.aspx>. [Accessed: 28-Apr-2016].
- [2] "3GPP: The Mobile Broadband Standard." *3GPP*. [Online]. Available: <http://www.3gpp.org/specifications/releases>. [Accessed: 08-Aug-2014].
- [3] "Request for Comments (RFC)". The Internet Engineering Task Force (IETF). [Online]. Available: 2014: <http://www.ietf.org/rfc.html>. [Accessed: 21-Feb-2014].
- [4] "IEEE Advancing Technology for Humanity." *IEEE*. [Online]. Available: <http://www.ieee.org/>. [Accessed: 21-Feb-2014].
- [5] "Open Mobile Alliance Mobile Phone Standards & Specifications | OMA." *OMA*. [Online]. Available: <http://openmobilealliance.org/>. [Accessed: 24-Mar-2014].
- [6] "GSM Association." *GSMA*. [Online]. Available: <http://www.gsma.com/>. [Accessed: 24-Mar-2014].
- [7] "TM Forum is a global, non-profit industry association focused on enabling service provider agility and innovation." *TM Forum*. [Online]. Available: <http://www.tmforum.org/>. [Accessed: 24-Mar-2014].
- [8] Erik Dahlman et al., *4G: LTE/LTE-Advanced for Mobile Broadband*, Oxford, United Kingdom, AP, 2011.

[9] Stefania Sesia et al., *LTE – The UMTS Long Term Evolution. From Theory to Practice*, 2nd Edition. Chippingham, Wiltshire, Great Britain: Wiley, 2011.

[10] “Ericsson Mobility Report.” Open Article. *Ericsson.com*, June, 2016. [Online]. Available: <https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf>. [Accessed: 19-Sept-2016].

[11] International Telecommunication Union (2015). *The World in 2015. ICT Facts and Figures. ITU Telecom World '15* [Online]. Available: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>. [Accessed: 28-Apr-2016].

[12] T. Russell, *Signaling system #7*. New York: McGraw-Hill, 2006.

[13] L. Dryburgh and J. Hewett, *Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services (Networking Technology)*, 1 edition. Cisco Press, 2004.

[14] G. Heine, *GSM networks: protocols, terminology, and implementation*. Boston, Mass.: Artech House, 1999.

[15] T. Halonen and J., Melero, Juan Romero, *GSM, GPRS, and EDGE performance evolution towards 3G/UMTS*. Chichester, West Sussex, England; Hoboken, NJ, USA: J. Wiley, 2003.

[16] A. Henry-Labordère, *Virtual roaming systems for GSM, GPRS, and UMTS: open connectivity in practice*. Chichester, West Sussex, U.K.; Hoboken, NJ: John Wiley, 2009.

[17] H. Kaaranen, *UMTS networks: architecture, mobility and services*. Chichester [etc.]: John Wiley & Sons, 2005.

[18] M. Etoh, *Next generation mobile systems: 3G and beyond*. Chichester, England; Hoboken, NJ: John Wiley, 2005.

[19] C. Kappler, UMTS networks and beyond. Chichester, U.K.: John Wiley & Sons, 2009.

[20] "METIS 2020," METIS 2020. [Online]. Available: <https://www.metis2020.com>. [Accessed: 04-Mar-2014].

[21] I. Juhasz, H. Schwarzbauer, and M. Holdrege, "Framework Architecture for Signaling Transport." [Online]. Available: <http://tools.ietf.org/html/rfc2719>. [Accessed: 21-Feb-2014].

[22] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) specification (Release 13), 3GPP TS 29.002 V13.3.0 (2016-03), 2016.

[23] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 4; CAMEL Application Part (CAP) specification (Release 13), 3GPP TS 29.078 V13.0.0 (2015-12), 2015.

[24] Rogier Noldus, CAMEL Intelligent Networks for the GSM GPRS and UMTS Networks, West Sussex, England, Wiley, 2006.

[25] International Telecommunication Union, Telecommunication Standardization Sector of ITU; ISDN user-network interface layer 3 specification for basic call control; ITU-T Recommendation Q.931; 1999.

[26] International Telecommunication Union, Telecommunication Standardization Sector of ITU; Bearer Independent Call Control protocol (Capability Set 2) Functional Description; ITU-T Recommendation Q.1902.1; 2001.

[27] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunneling Protocol (GTP) User Plane (GTPv1-U) (Release 13); 3GPP TS 29.281 V13.1.0 (2016-03), 2016.

[28] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3 (Release 13); 3GPP TS 29.274 V13.5.0 (2016-13), 2016.

[29] E. Schooler, G. Camarillo, M. Handley, J. Peterson, J. Rosenberg, A. Johnston, H. Schulzrinne, and R. Sparks, "SIP: Session Initiation Protocol." IETF RFC 3261, Jun. 2002.

[30] A. B. Johnston, SIP understanding the Session Initiation Protocol, third edition. Norwood, Mass.: Artech House, 2009.

[31] J. Arkko, G. Zorn, V. Fajardo, and J. Loughney, "Diameter Base Protocol." IETF RFC 6733, Oct. 2012.

[32] M. Nakhjiri and M. Nakhjiri, AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility. Chichester, England; Hoboken, NJ: John Wiley & Sons, 2005.

[33] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 13), 3GPP TS 23.228 V13.5.0 (2016-03), 2016.

[34] Gonzalo Camarillo and Miguel A. García-Martín, *The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the Cellular Worlds*, 3rd. ed., West Sussex, England, Wiley, 2008.

[35] Rogier Noldus et al., IMS Application Developer's Handbook Creating and Deploying Innovative IMS Applications, Oxford, United Kingdom, AP, 2011.

[36] "El Ministerio TIC publica resultados del estudio para la Red Nacional de Telecomunicaciones de Emergencia - Ministerio de Tecnologías de la Información y las Comunicaciones." [Online]. Available: <http://www.mintic.gov.co/portal/604/w3-article-4386.html>. [Accessed: 28-Apr-2016].



[37] International Telecommunication Union, Development Standardization Sector of ITU (2012). *Fortalecimiento de las TIC para Emergencias*. [Online]. Available: [https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Bogota\\_2012/presentation/PresentationViveDigitalSp.pdf](https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Bogota_2012/presentation/PresentationViveDigitalSp.pdf). [Accessed: 28-Apr-2016].

[38] Comisión de Regulación de Comunicaciones, República de Colombia. (2013, Oct. 10). *Promoción de servicios financieros sobre redes móviles y medidas complementarias para provisión de contenidos y aplicaciones* [Online]. Available: [http://www.crcm.gov.co/uploads/images/files/DocSoporte\\_SFM.pdf](http://www.crcm.gov.co/uploads/images/files/DocSoporte_SFM.pdf). [Accessed: 28-Apr-2016].

[39] Digital cellular telecommunications system (Phase 2+); Unstructured Supplementary Service Data (USSD) - Stage 1 (GSM 02.90 version 7.0.0 Release 1998), ETSI TS 100 625 V7.0.0 (1999-08), 1999.

[40] Digital cellular telecommunications system (Phase 2+); Unstructured Supplementary Service Data (USSD) - Stage 2 (GSM 03.90 version 7.0.0 Release 1998), ETSI TS 100 549 V7.0.0 (1999-08), 1999.

[41] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Unstructured Supplementary Service Data (USSD); Stage 3 (Release 13), 3GPP TS 24.090 V13.0.0 (2015-12), 2015.

[42] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Unstructured Supplementary Service Data (USSD) using IP Multimedia (IM) Core Network (CN) subsystem IMS; Stage 3 (Release 13), 3GPP TS 24.390 V13.0.0 (2015-12), 2015.

[43] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Location Services (LCS); LCS Application Protocol (LCS-AP) between the Mobile Management Entity (MME) and Evolved Serving Mobile Location Centre (E-SMLC); S<sub>L</sub>s interface (Release 13), 3GPP TS 29.171 V13.2.0 (2016-03), 2016.

[44] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Location Services (LCS); Evolved Packet Core (EPC) LCS Protocol (ELP) between the Gateway Mobile Location Centre (GMLC) and the Mobile Management Entity (MME); SL<sub>g</sub> interface (Release 13), 3GPP TS 29.172 V13.0.0 (2016-01), 2016.

[45] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Location Services (LCS); Diameter-based SL<sub>h</sub> interface for Control Plane LCS (Release 13); 3GPP TS 29.173 V13.0.0 (2015-12), 2015.

[46] Jürgen Kress, Berthold Maier, Hajo Normann, Danilo Schmeidel, Guido Schmutz, Bernd Trops, Clemens Utschig-Utschig, and Torsten Winterberg. (2013, Jul.). *Industrial SOA* [Online]. Available: <http://www.oracle.com/technetwork/articles/soa/ind-soa-toc-1934143.html>.

[47] “IBM - What is SOA?” 19-Feb-2014. [Online]. Available: <http://www-01.ibm.com/software/solutions/soa/what-is-soa.html>. [Accessed: 25-Feb-2014].

[48] “USSD 2.0 Redux - 3GPP IMS Release-11 calls it USSI,” *Aayush: weblog*.

[49] G. Suddul, A. Soobul, U. Bahadoor, A. Ramdoyal, N. Doolhur, and M. Richomme, “An Open USSD Enabler to Simplify Access to Mobile Services in Emerging Countries,” in 2011 4th International Conference on Emerging Trends in Engineering and Technology (ICETET), 2011, pp. 323–326.

[50] A. Sarajlic and D. Omerasevic, “Access Channels in m-Commerce Services,” in 29th International Conference on Information Technology Interfaces, 2007. ITI 2007, 2007, pp. 507–512.

[51] D. Bogusz, J. Legierski, A. Podziewski, and K. Litwiniuk, “Telco 2.0 for UC #x2014; An example of integration telecommunications service provider’s SDP with enterprise UC system,” in 2012 Federated Conference on Computer Science and Information Systems (FedCSIS), 2012, pp. 603–606.

[52] Janagoudar Sanganagouda, Aricent Group (2011, Sept.), *USSD: A Communication Technology to Potentially Ouster SMS Dependency*. [Online]. Available: [http://www.aricent.com/files/pdf/Aricent\\_WhitePaper\\_USSD\\_0911.pdf](http://www.aricent.com/files/pdf/Aricent_WhitePaper_USSD_0911.pdf). [Accessed: 21-Feb-2014].

[53] I. Sato, A. Bouabdallah, and X. Lagrange, "A New LTE/EPC Control-Plane Based Transmission Procedure to Cope with Short Data Push Services," *Wireless Pers Commun*, vol. 72, no. 3, pp. 1723–1735, Oct. 2013.

[54] M. Ficek, T. Pop, and L. Kencl, "Active tracking in mobile networks: An in-depth view," *Computer Networks*, vol. 57, no. 9, pp. 1936–1954, Jun. 2013.

[55] M. GhasemiNajm, M. J. N. Sibley, and A. Jafarian, "Combination of LTE and IMS to deliver location based services," in *Telecommunications Forum (TELFOR)*, 2012 20th, 2012, pp. 56–59.

[56] Persistent Systems Ltd., "Whitepaper – Delivering Location in LTE Networks." 2011.

[57] Ericsson. (2011, Sept.), *Positioning in LTE - Ericsson White paper 284 23-3155 Sep-2011*. [Online]. Available: <http://www.sharetechnote.com/Docs/WP-LTE-positioning.pdf>. [Accessed: 28-Apr-2016].

[58] Ericsson. (2011, Sept.), *Positioning in LTE - Ericsson White paper 284 23-3155 Sep-2011*. [Emphasis added.] LTE Positioning Architecture, Protocol and Methods [Online]. Available: <http://apps.fcc.gov/ecfs/document/view?id=7021905643>. [Accessed: 28-Apr-2016].

[59] MultiService Forum (2009), *MSF Whitepaper on Location Services in LTE Networks*. [Online]. Available: <http://www.msforum.org/techinfo/reports/MSF-TR-SERVICES-005-FINAL.pdf>. [Accessed: 28-Apr-2016].

[60] Sven Fischer (2014, June, 6). Observed Timed Difference of Arrival Positioning (OTDOA) in 3GPP LTE. Qualcomm Technologies Inc. [Online]. Available:

<http://www.qualcomm.com/media/documents/files/otdoa-positioning-in-3gpp-lte.pdf>.  
[Accessed: 28-Apr-2016].

[61] Broadcom (2007, Oct.), *Secure User Plane Location*. [Online]. Available: <http://www.broadcom.com/collateral/wp/SUPL-WP100-R.pdf>. [Accessed: 28-Apr-2016].

[62] Open Mobile Alliance; User Plane Location Protocol, OMA-TS-ULP-V2\_0\_1-20121205-A; 2012. [Online]. Available: [http://technical.openmobilealliance.org/Technical/release\\_program/docs/SUPL/V2\\_0\\_1-20121205-A/OMA-TS-ULP-V2\\_0\\_1-20121205-A.pdf](http://technical.openmobilealliance.org/Technical/release_program/docs/SUPL/V2_0_1-20121205-A/OMA-TS-ULP-V2_0_1-20121205-A.pdf). [Accessed: 28-Apr-2016].

[63] S. S. Cherian and A. N. Rudrapatna, "LTE Location Technologies and Delivery Solutions," *Bell Labs Tech. J.*, vol. 18, no. 2, pp. 175–194, Sep. 2013.

[64] P. Reichl, S. Bessler, J. Fabini, R. Pailer, A. Poropatich, N. Jordan, R. Huber, H. Weisgrab, C. Brandner, I. Gojmerac, M. Ries, and F. Wegscheider, "Practical Experiences with an IMS-aware Location Service Enabler on Top of an Experimental Open Source IMS Core Implementation," *J. Mob. Multimed.*, vol. 2, no. 3, pp. 189–224, Sep. 2006.

[65] A. MacDonald, R. Cartas, and J. Incera, "Custom tailored location based services: An IMS implementation," in 2011 18th International Conference on Telecommunications (ICT), 2011, pp. 118–123.

[66] H. Schmidt, T. Guenkova-Luy, and F. J. Hauck, "Service Location using the Session Initiation Protocol (SIP)," in *International conference on Networking and Services, 2006. ICNS '06*, 2006, pp. 60–60.

[67] M. Salem, P. Ruppel, U. Bareth, and A. Kupper, "X-centric positioning: A combination of device-centric and multi-rat network-centric positioning approaches in NGN," in *2012 IEEE Globecom Workshops (GC Wkshps)*, 2012, pp. 1741–1746.

[68] David Ferry, Open Cloud, Sun Microsystems Inc. (2008). *JSR-000240 JAIN SLEE (JSLEE) 1.1 Specification Final Release* Available:

<https://jcp.org/aboutJava/communityprocess/final/jsr240/index.html>. [Accessed: 28-Apr-2016].

[69] Mobicents (2008). [Online]. Available: <http://www.mobicents.org>. [Accessed: 17-Jul-2014].

[70] Z. Shicheng, H. Xiaoxiao, C. Bo, and C. Junliang, "The design and implementation of component-based multimedia conferencing services model," in *2nd IEEE International Conference on Broadband Network Multimedia Technology, 2009. IC-BNMT '09*, 2009, pp. 132–136.

[71] C. Bo, Z. Yang, Z. Peng, D. Hua, H. Xiaoxiao, W. Zheng, and C. Junliang, "Development of Web-Telecom Based Hybrid Services Orchestration and Execution Middleware over Convergence Networks," *J. Netw. Comput. Appl.*, vol. 33, no. 5, pp. 620–630, Sep. 2010.

[72] C. Bo, C. Junliang, and D. Min, "Petri Net Based Formal Analysis for Multimedia Conferencing Services Orchestration," *Expert Syst. Appl.*, vol. 39, no. 1, pp. 696–705, Jan. 2012.

[73] F. A. Leitão, S. S. Freire, and S. R. Lima, "SMS over LTE: Interoperability between legacy and Next Generation Networks," in *2010 IEEE Symposium on Computers and Communications (ISCC)*, 2010, pp. 634–639.

[74] Filipe Alexandre Rodrigues de Moura Leitão, "Cenários de convivência de serviços de mensagens entre redes tradicionais e redes de próxima geração," Universidade do Minho, Portugal, 2009.

[75] Balefyre. (2013, June). *BFDS-20136311/R2 - USSDX™ V.2* [Online]. Available: <http://www.balefyre.co.za/pdfs/usssdx.pdf>. [Accessed: 23-Sep-2014].

[76] Mobicents (2008), "USSD Gateway - Mobicents". [Online]. Available: <http://www.mobicents.org/incubator/usssd/intro.html>. [Accessed: 26-Feb-2014].

[77] "TelScale USSD Gateway 6.2.0.GA is now available!" TeleStax. [Online]. Available: <https://telestax.com/telscale-ussd-gateway-6-2-0-ga/>. [Accessed: 28-Apr-2016].

[78] Alcatel-Lucent. (2009), *Options for Providing Voice over LTE and Their Impact on the GSM/UMTS Network*. [Online]. Available: [http://www3.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG\\_CABINET=Docs\\_and\\_Resource\\_Ctr&LMSG\\_CONTENT\\_FILE=White\\_Papers/CPG1649091001\\_Options\\_for\\_Providing\\_Voice\\_as\\_LTE\\_is\\_Introduced\\_EN\\_StraWhitePaper.pdf](http://www3.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=White_Papers/CPG1649091001_Options_for_Providing_Voice_as_LTE_is_Introduced_EN_StraWhitePaper.pdf). [Accessed: 28-Apr-2016].

[79] Ericsson. (2013, January). What is voice over LTE? [Online]. Available: [http://www.ericsson.com/res/thecompany/docs/press/backgrounders/volte\\_pressbackgrunder.pdf](http://www.ericsson.com/res/thecompany/docs/press/backgrounders/volte_pressbackgrunder.pdf). [Accessed: 28-Apr-2016].

[80] Ericsson. (2012, Feb.), Voice and Video Calling over LTE - Ericsson White paper 284 23-3163 Uen. [Online]. Available: <http://www.ericsson.com/res/docs/whitepapers/WP-Voice-Video-Calling-LTE.pdf>. [Accessed: 28-Apr-2016].

[81] Mobicents Google Public Group. (2013, Dec., 14). "Re: [mobicents-public] Mobicents Diameter implementation". [Online]. Available: [https://groups.google.com/forum/#!msg/mobicents-public/lxpMDrBqBkA/\\_2ok6\\_1Zq6sJ](https://groups.google.com/forum/#!msg/mobicents-public/lxpMDrBqBkA/_2ok6_1Zq6sJ). [Accessed: 28-Apr-2016].

[82] J. A. Rojas Meléndez, J. D. Ramírez, and J. C. Corrales, "Soa-Based Guidelines for Value-Added Service Development on Jain SLEE Environments," *Revista Ingenierías Universidad de Medellín*, 2012. [Online]. Available: <http://www.redalyc.org/resumen.oa?id=75025842014>. [Accessed: 28-Apr-2016].

[83] Open Source IMS Core. (2008). *Welcome to Open IMS Core's Homepage*. [Online]. Available: <http://www.openimscore.org/>. [Accessed: 05-Aug-2014].

[84] Core Network Dynamics, Fraunhofer Institute for Open Communication Systems FOKUS. (2013). *OpenEPC The OpenEPC Project*. [Online]. Available: <http://www.openepc.com/>. [Accessed: 28-Apr-2016].

[85] T. Q. Thanh, D. Vingarzan, Y. Rebahi, and T. Magedanz, "A Diameter based testing system in Next Generation Mobile Network," in *Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International*, 2010, pp. 1–5.

[86] OpenLTE. (2014). *OpenLTE is an open source implementation of the 3GPP LTE specifications*. [Online]. Available: <http://openlte.sourceforge.net/>. [Accessed: 28-Apr-2016].

[87] G. Piro, L. A. Grieco, G. Boggia, F. Capozzi, and P. Camarda, "Simulating LTE Cellular Systems: An Open-Source Framework," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 498–513, Feb. 2011.

[88] G. Piro, "LTE-Sim - the LTE simulator," [OnLine] Available: <http://telematics.poliba.it/LTE-Sim>. [Accessed: 28-Apr-2016].

[89] "Vienna LTE-A Simulators." [Online]. Available: <https://www.nt.tuwien.ac.at/research/mobile-communications/vienna-lte-a-simulators/>. [Accessed: 28-Apr-2016].

[90] OpenBTS. (2014). OpenBTS.org. [Online]. Available: <http://openbts.org/>. [Accessed: 28-Apr-2016].

[91] "Performance Evaluation of GSM Signaling Protocols on USSD: ComNets Research Group." [Online]. Available: [http://www.comnets.rwth-aachen.de/index.php?id=6443&tx\\_cndownload\\_pi1%5Bpubtype%5D=Download&tx\\_cndownload\\_pi1%5Buid%5D=189](http://www.comnets.rwth-aachen.de/index.php?id=6443&tx_cndownload_pi1%5Bpubtype%5D=Download&tx_cndownload_pi1%5Buid%5D=189). [Accessed: 15-May-2016].

[92] Agencia Noruega para la Cooperación para el Desarrollo (NORAL). "Enfoque del marco lógico (EML) como herramienta para planificación y gestión de proyectos orientados por objetivos". 1a. Ed. Española, Instituto Universitario de

Desarrollo y Cooperación, Madrid, 1993. [En línea] Publicado por la Universidad Complutense de Madrid: <http://www.ucm.es/info/ucmp/cont/descargas/documento26378.pdf>.

[93] “Research and Development Centre for Mobile Applications (RDC).” [Online]. Available: <http://www.rdc.cz/en/aboutUs/>. [Accessed: 28-Apr-2016].

[94] “Fraunhofer Institute for Open Communication Systems FOKUS.” [Online]. Available: <https://www.fokus.fraunhofer.de/en>. [Accessed: 28-Apr-2016].

[95] “Bell Labs.” [Online]. Available: <http://www.alcatel-lucent.com/bell-labs>. [Accessed: 28-Apr-2016].

[96] “Telekom Innovation Laboratories.” [Online]. Available: <http://www.laboratories.telekom.com/public/English/Pages/default.aspx>. [Accessed: 28-Apr-2016].

[97] “The Telecommunications Research Centre Vienna (FTW).” Available: [http://www.ftw.at/?set\\_language=en](http://www.ftw.at/?set_language=en). [Accessed: 28-Apr-2016].

[98] “Nethalis - Servicios de Valor Añadido y Soluciones M2M.” [Online]. Available: [http://www.nethalis.com/esp/VAS\\_2.htm](http://www.nethalis.com/esp/VAS_2.htm). [Accessed: 28-Apr-2016].

[99] Mobicents Google Public Group. (2014, Oct., 31). “[mobicents-public] Mobicents Diameter v1.6.0.FINAL Released!”. [Online]. Available: [https://groups.google.com/forum/#!searchin/mobicents-public/Mobicents\\$20Diameter\\$20v1.6.0.FINAL\\$20Released!/mobicents-public/AG\\_Fn6EUQ28/joZeW6DeoxUJ](https://groups.google.com/forum/#!searchin/mobicents-public/Mobicents$20Diameter$20v1.6.0.FINAL$20Released!/mobicents-public/AG_Fn6EUQ28/joZeW6DeoxUJ). [Accessed: 02-Nov-2014].

[100] B. Kitchenham, S. Linkman, and D. Law, “DESMET: a methodology for evaluating software engineering methods and tools,” *Computing Control Engineering Journal*, vol. 8, no. 3, pp. 120–126, Jun. 1997.

[101] “Rational Unified Process Best Practices for Software Development Teams Rational Software White Paper TP026B, Rev 11/01.” Rational, the Software



Development Company, Nov-2001. [Online]. Available: [https://www.ibm.com/developerworks/rational/library/content/03July/1000/1251/1251\\_bestpractices\\_TP026B.pdf](https://www.ibm.com/developerworks/rational/library/content/03July/1000/1251/1251_bestpractices_TP026B.pdf). [Accessed: 03-Dec-2014].

[102] "Extreme Programming: A Gentle Introduction." [Online]. Available: <http://www.extremeprogramming.org/>. [Accessed: 03-Dec-2014].

[103] "Scrum.org | The home of Scrum > Home." [Online]. Available: <https://www.scrum.org/>. [Accessed: 03-Dec-2014].

[104] "The 5G Infrastructure Public Private Partnership" 5G-PPP. [Online]. Available: <https://5g-ppp.eu>. [Accessed: 28-Apr-2014].

[105] "NG9-1-1 Project - National Emergency Number Association." [Online]. Available: [http://www.nena.org/?NG911\\_Project](http://www.nena.org/?NG911_Project). [Accessed: 01-May-2016].

[106] "Ley Stalker: PNP Y Empresas Firman Protocolo de Geolocalización." El Comercio, October 16, 2015. <http://elcomercio.pe/lima/seguridad/geolocalizacion-celulares-pnp-y-operadoras-firman-protocolo-noticia-1848628>.

[107] Open Mobile Alliance; Mobile Location Protocol (MLP); OMA-LIF-MLP-V3\_1-20110920-A Approved Version 3.1 – 20 Sep 2011. [Online]. Available: <http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/mlp-v3-1>. [Accessed: 2-May-2016].

[108] Open Mobile Alliance; User Plane Location Protocol; OMA-TS-ULP-V3\_0-20140916-C; Candidate Version 3.0 – 16 Sep 2014. [Online]. Available: <http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/secure-user-plane-location-v3-0>. [Accessed: 2-May-2016].

[109] "Restcomm - the #1 Telephony App Server." Restcomm. Accessed May 2, 2016. [Online]. Available: <http://www.restcomm.com/>. [Accessed: 2-May-2016].

[110] "Real Time Communication Unleashed." Telestax. [Online]. Available: <https://telestax.com/>. [Online]. [Accessed: 28-Apr-2016].

[111] “Building USSD Apps for Restcomm - Part 1.” Telestax, February 20, 2014. [Online]. Available: <https://telestax.com/building-ussd-apps-restcomm-part-1/>. [Accessed: 28-Apr-2016].

[112] “Building USSD Apps for Restcomm - Part 2 - USSD Push.” *Telestax*, March 14, 2014. [Online]. Available: <https://telestax.com/building-ussd-apps-restcomm-part-2/>. [Accessed: 28-Apr-2016].

[113] Adusei, I. K., K. Kyamakya, and K. Jobmann. “Mobile Positioning Technologies in Cellular Networks: An Evaluation of Their Performance Metrics.” In *MILCOM 2002. Proceedings*, 2:1239–44 vol.2, 2002. doi:10.1109/MILCOM.2002.1179656.

[114] DeanB. “Disruptive Analysis.” *Dean Bublely & Disruptive Analysis*. [Online]. Available: <http://www.deanbublely.com/disruptive-analysis/>. [Accessed: 28-Apr-2016].

[115] Chaesub Lee. (2009, May 08). Architectural Overview of ITU-T NGN (including Future Vision) [Online]. Available: <http://www.itu.int/ITU-T/worksem/ngn/200905/>. [Accessed: 15-May-2016].

[116] Salmiah Abd Majid. (2009, April 09). Telekom Malaysia’s NGN Implementation Plan [Online]. Available: <http://www.itu.int/ITU-T/worksem/ngn/200904/programme.html>. [Accessed: 15-May-2016].

[117] “Telefónica Global CIO: Telecoms Must Change to Survive.” *RCR Wireless News*, May 20, 2015. [Online]. Available: <http://www.rcrwireless.com/20150520/americas/telefonicas-global-cio-it-has-become-core-differentiation-and-telecoms-must-change-to-survive-tag5>. [Accessed: 15-May-2016].

[118] Muhammad Suhaizan Sulong, Andy Koronios, Jing Gao, and Azliyanor Abdul-Aziz. “Driving the Initiative of Service-Oriented Architecture Implementation.”

Journal of Software & Systems Development 2012 (n.d.): 10.  
doi:10.5171/2012.169423.

[119] Fernando Mendioroz Cotelo, Álvaro Rendón-Gallón, Juan Carlos Corrales-Muñoz, and Julián Andrés Rojas-Meléndez. "Challenges of SOA Adoption in the Telco Domain for Latin American Researchers." *Facultad de Ingeniería* 24, no. 39 (May 5, 2015): 9–19.

[120] "Alan Quayle - Business and Service Development." *Alan Quayle Business and Service Development*. [Online]. Available: <http://alanquayle.com/>. [Accessed: 15-May-2016].

[121] "Project Clearwater." Metaswitch Networks. [Online]. Available: <http://www.projectclearwater.org/>. [Accessed: 15-May-2016].

[122] "TeleStax Open Source Playbook." *Google Docs*. [Online]. Available: [https://docs.google.com/a/telestax.com/document/d/1RZz2nd2ivCK\\_rg1vKX9ansgNF6NpK\\_PZI81GxZ2MSnM/edit?usp=drive\\_web&usp=docs\\_home&ths=true&usp=embed\\_facebook](https://docs.google.com/a/telestax.com/document/d/1RZz2nd2ivCK_rg1vKX9ansgNF6NpK_PZI81GxZ2MSnM/edit?usp=drive_web&usp=docs_home&ths=true&usp=embed_facebook). [Accessed: 15-May-2016].

[123] "Q.9: Vocabulary of Switching and Signalling Terms." [Online]. Available: <https://www.itu.int/rec/T-REC-Q.9-198811-l/en>. [Accessed: 8-August-2016].

[124] "CEPT.ORG - ECC." [Online]. Available: <http://www.cept.org/ECC>. [Accessed: 8-August-2016].

[125] Quayle, Alan. "TADHack-Mini Chicago Winners." Blog @ TADHack - Telecom Application Developer Hackathon, October 4, 2015. [Online]. Available: <http://blog.tadhack.com/2015/10/04/tadhack-mini-chicago-winners/>. [Accessed: 8-August-2016].

[126] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional stage 2 description of Location Services (LCS) (Release 13), 3GPP TS 23.271 V13.0.0 (2015-09), 2015.

[127] Cisco Systems. (2009). *Introduction to eTOM White Paper* [Online]. Available: [http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white\\_paper\\_c11-541448.pdf](http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-541448.pdf). [Accessed: 23-Sep-2014].

[128] Mourabit, I. E., A. Badri, A. Sahel, and A. Baghdad. "Enhanced Mobile Positioning Technique for UMTS Users in Both Outdoor and Indoor Environments." In 2014 Third IEEE International Colloquium in Information Science and Technology (CIST), 335–39, 2014. doi:10.1109/CIST.2014.7016642.

[128] "The RestComm Open Source Project on Open Hub." [Online]. Available: <https://www.openhub.net/p/restcomm>. [Accessed: 11-Sep-2016].

[129] "Analysis Summary." [Online]. Available: <http://ci.telestax.com/view/Telscale-SS7/job/Telscale-gmlc-Performance-GetLoc/113/artifact/results/PerfCorderAnalysis.html>. [Accessed: 30-Oct-2016].

[130] SLg interface implementation #37 by FerUy · RestComm/jdiameter." GitHub. [Online]. Available: <https://github.com/RestComm/jdiameter/issues/37>. [Accessed: 21-Oct-2016].

[131] SLh interface implementation #38 by FerUy · RestComm/jdiameter." GitHub. [Online]. Available: <https://github.com/RestComm/jdiameter/issues/38>. [Accessed: 21-Oct-2016].

[132] "LTE Location Services by FerUy · Pull Request #48 · RestComm/jdiameter." GitHub. [Online]. Available: <https://github.com/RestComm/jdiameter/pull/48>. [Accessed: 21-Oct-2016].

[133] "Telecom Application Developer Summit (TADS) 2016." *Telecom Application Developer Summit 2016*. [Online]. Available: <http://tadsummit.com/2016/>. [Accessed: 18-Oct-2016].

[134] "RestComm/jain-Slee.diameter." *GitHub*. [Online]. Available: <https://github.com/RestComm/jain-slee.diameter>. [Accessed: 21-Oct-2016].

[135] Juan Carlos Corrales Muñoz, Oscar Mauricio Caicedo Rendón, Francisco Orlando Martínez Pabón, Javier Orlando Hurtado Guaca, Julián Andrés Rojas Meléndez, *Tecnologías para el Desarrollo de Servicios Convergentes*, Universidad del Cauca, Colombia, 2011.

[136] “WebRTC 1.0: Real-Time Communication Between Browsers.” [Online]. Available: <http://w3c.github.io/webrtc-pc/>. [Accessed: 06-Nov-2016].

[137] Castillo, Inaki Baz, Victor Pascual, and Jose Luis Millan Villegas. “The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP).” [Online]. Available: <https://tools.ietf.org/html/rfc7118>. IETF RFC 7118. [Accessed: 06-Nov-2016].

[138] “JSR 359: SIP Servlet 2.0 (The Aquarium).” [Online]. Available: [https://blogs.oracle.com/theaquarium/entry/jsr\\_359\\_sip\\_servlet\\_2](https://blogs.oracle.com/theaquarium/entry/jsr_359_sip_servlet_2). [Accessed: 06-Nov-2016].

[139] Davids,C., Moreno Valdecantos, J.,Dworak, B.,Tovar, C., Ramaswamy Nandakumar, B., Patil, M. "Dispatchable Indoor Location for Mobile Phones Calling for Emergency Services," In Proceedings of the 8th ACM International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm 2015), pp. 22-27, Chicago, Illinois, Oct., 2015.

[140] “Git.” [Online]. Available: <https://git-scm.com/>. [Accessed: 06-Nov-2016].

[141] “Build Software Better, Together.” GitHub. [Online]. Available: <https://github.com>. [Accessed: 06-Nov-2016].

[142] Oscar R. Pons. “Introducción a las Telecomunicaciones fijas y móviles”, Tapias Encuadernaciones. Argentina. 2014.

[143] “SLh RA Implementation · Issue #15 · RestComm/jain-Slee.diameter.” GitHub. [Online]. Available: <https://github.com/RestComm/jain-slee.diameter/issues/15>. [Accessed: 14-Nov-2016].

[144] "SLg RA Implementation · Issue #16 · RestComm/jain-Slee.diameter." GitHub. [Online]. Available: <https://github.com/RestComm/jain-slee.diameter/issues/16>. [Accessed: 14-Nov-2016].

[145] Abd Majid, S. "NGN Implementation Guideline". Awareness Seminar on Telecommunication Standards & Practices. Cyberjaya, Malaysia. 2009.

[146] Sushant et al. "NGN: Next Generation Network". Regional Telecom Training Centre Rajpura, India. E-Magazine. 2010.

## Extended Bibliography

[E1] 3rd Generation Partnership Project; Universal Mobile Telecommunications System (UMTS); (3GPP TS 25.301 version 7.5.0 Release 7).

[E2] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2 (Release 12) (3GPP TS 23.060 V12.1.0 (2013-06)).

[E3] "Locatrix Communications | Mobile App Development, Managed Services, Web Services, Telecommunications." [Online]. Available: <http://www.locatrix.com/>. [Accessed: 18-Oct-2016].

[E4] "International Mobile Business Calls | Truphone UK." [Online]. Available: <https://www.truphone.com/uk/>. [Accessed: 18-Oct-2016].

[E5] "American Prepaid VAS | Helping Carriers to Make Money." [Online]. Available: <http://americanprepaidvas.com/>. [Accessed: 18-Oct-2016].

[E6] "Restcomm API - Geolocation". [Online]. Available: <http://documentation.telestax.com/connect/api/geolocation-api.html>. [Accessed: 4-Nov-2016].

[E7] "Restcomm RCML - Geolocation". [Online]. Available: <http://documentation.telestax.com/connect/rcml/geolocation-rcml.html>. [Accessed: 4-Nov-2016].

[E8] "User Guide to Restcomm GMLC." [Online]. Available: [http://documentation.telestax.com/core/gmlc/GMLC\\_Admin\\_Guide.html](http://documentation.telestax.com/core/gmlc/GMLC_Admin_Guide.html). [Accessed: 28-Oct-2016].

[E9] “Analysis Summary.” [Online]. Available: <http://ci.telestax.com/view/Telscale-SS7/job/Telscale-gmlc-Performance-GetLoc/99/artifact/results/PerfCorderAnalysis.html>. [Accessed: 18-Oct-2016].

[E10] “Agenda for RestConn 2015.” *Telestax*, October 15, 2015. [Online]. Available: <https://telestax.com/agenda-for-restconn-2015/>. [Accessed: 18-Oct-2016].

[E11] “Location Based Services at Heterogeneous Networks.” 15:23:19 UTC. [Online]. Available: <http://www.slideshare.net/telestax/location-based-services-at-heterogeneous-networks>. [Accessed: 18-Oct-2016].

[E12] “Locatrix Communications | Mobile App Development, Managed Services, Web Services, Telecommunications.” [Online]. Available: <http://www.locatrix.com/>. [Accessed: 18-Oct-2016].

[E13] “International Mobile Business Calls | Truphone UK.” [Online]. Available: <https://www.truphone.com/uk/>. [Accessed: 18-Oct-2016].

[E14] Ivanov, Ivelin. “@FerMendioroz Is Laying the Roadmap for #Restcomm Location APIs. Happy to Have @mark\_locatrix and @jamesbody at This Pivotal Discussion.” Microblog. @ivelini, November 21, 2015. <https://twitter.com/ivelini/status/668051679879778304?cn=ZmF2b3JpdGVfbWVudGlvbWVkX3VzZXI%3D&refsrc=email>.

[E15] White, Mark. “Thanks to #restconn15 I’m More Excited by Mobile LBS Applications than I Have Been in YEARS. Kudos to @telestax + @jamesbody @FerMendioroz.” Microblog, November 21, 2015. <https://twitter.com/search?q=%23restconn15&cn=ZmF2b3JpdGVfbWVudGlvbWVkX3VzZXI%3D&refsrc=email>.

[E16] Body, James. “An Awesome Presentation - Loved the Animations! Much Respect to @FerMendioroz for Attention to detail!!<https://twitter.com/deruelle/status/668056250773565441> ....” Microblog.



@jamesbody, November 23, 2015.  
<https://twitter.com/jamesbody/status/668792543925137408?refsrc=email>.

[E17] "TUCAN3G @ Enlace Hispano Americano de Salud." [Online]. Available: <http://www.ahas.org/que-hacemos/investigacion-y-desarrollo/tucan3g/>. [Accessed: 8-Nov-2016].

[E18] "TUCAN3G Project Summary." [Online]. Available: <http://www.ict-tucan3g.eu/>. [Accessed: 8-Nov-2016].

[E19] "The RestComm Open Source Project on Open Hub." [Online]. Available: <https://www.openhub.net/p/restcomm>. [Accessed: 8-Nov-2016].

[E20] "Restcomm Reaches An Impressive Growth Milestone." Telestax, May 4, 2016. [Online]. Available: <https://telestax.com/restcomm-reaches-impressive-growth-milestone/>. [Accessed: 5-May-2016].

[E21] "TADHack 2016 - Telecom Application Developer Hackathon." *TADHack 2016*. [Online]. Available: <http://tadhack.com/2016/>. [Accessed: 18-Oct-2016].

[E22] Quayle, Alan. "TADHack-Mini Uruguay 2016 Summary." Blog @ TADHack - Telecom Application Developer Hackathon, May 11, 2016. [Online]. Available: <http://blog.tadhack.com/2016/05/11/tadhack-mini-uruguay-2016-summary/>. Accessed: 10-Nov-2016].



## **Annex A**

# **A Signaling System N°7**

### **A.1 Introduction to SS7**

As for ITU-T Q.9 specification, signaling is defined as the exchange of information (other than by speech) specifically concerned with the establishment, release and other control of calls and network management in automatic telecommunications operation. Signaling commitment is providing a mechanism to transfer control information between nodes of a telecommunications system. Hence, through signaling, the set of information exchanged between two points of a telecommunications network (user-core or core-core) allows the following features:

- Supervision (state condition or change detection);
- Traffic Control;
- Routing (services establishment/release);
- Database access;
- OA&M: Network Operation, Administration and Maintenance;

#### **A.1.1 History**

ITU-T (formerly known as CCITT) became the standardization organization for signaling systems to be used in international communications. In 1934, CCITT began this labour by launching Signaling System N°1 or SS1. SS1 is a low-level type supervision bidirectional signaling protocol, using a single tone of 500 Hz modulated at a 20 Hz rate for call selection between switchboards. It entailed the international equivalent of Bell's 1000/20 Hz manual ringdown signaling.

By 1938, CCITT specified SS2 for semi-automatic services, although it was never used internationally. It consisted of two-tone (600/750 Hertz) system for dial-pulsing selection information. By 1954, SS3 recommendation is released. A single-frequency tone at 2280 Hertz was used on one-way circuits only either for line or register signaling. SS4 also emerges by 1954, widely used in Europe for international transit and terminal traffic within analog networks. Dual-tone at 2040 and 2400 Hz, it's considered the first truly global «direct dialing» signaling system.

By 1964, CCITT specifies SS5 for wire and satellite international connections. It's a two-tone (2400 and 2600 Hertz) system combined with multifrequency inter-register signaling for both terminal and transit traffic at 700, 900, 1100, 1300, 1500 and 1700 Hz. When multifrequency signaling began, pulse code modulation systems were discriminated from obliged signals systems like the one used by SSR2. While in the former systems the signal has a fixed and determined period, in the latter, at every step of the message, a confirmation response is expected on the return channel to stop the signal forward.

SS6 is defined as a common digital data path between two switching exchanges to negotiate and oversee connection control on transmission facility trunks between exchanges.

Signaling System N<sup>o</sup> 7 or Common Channel Signaling System No. 7 (SS7 according to ITU-T or CC7 according to ANSI), began in 1980 by CCITT (now ITU-T), published in Q.7nn recommendation series. SS7 comprises a global standard for telecommunications circuit-switched core networks, conveyed within Pulse Code Modulation (PCM) digital links.

SS7 defines the procedures and protocols for information exchange between signaling network entities for data and speech:

- Supervision
- Control
- Database access
- Management
- Routing

These definitions are also embraced by regional variants such as the likes of the American National Standards Institute (ANSI) & Bell Communications Research (Telcordia Technologies), as well as the European Telecommunications Standards Institute (ETSI).

## A.1.2 Types of signaling

### A.1.2.1 Channel Associated Signaling (CAS)

As for ITU-T Q.9, Channel Associated Signaling is a signaling method in which the signals needed for the traffic carried by a single channel are transmitted in the channel itself or in a signaling channel permanently dedicated to it. Each voice channel has its own associated signaling channel.

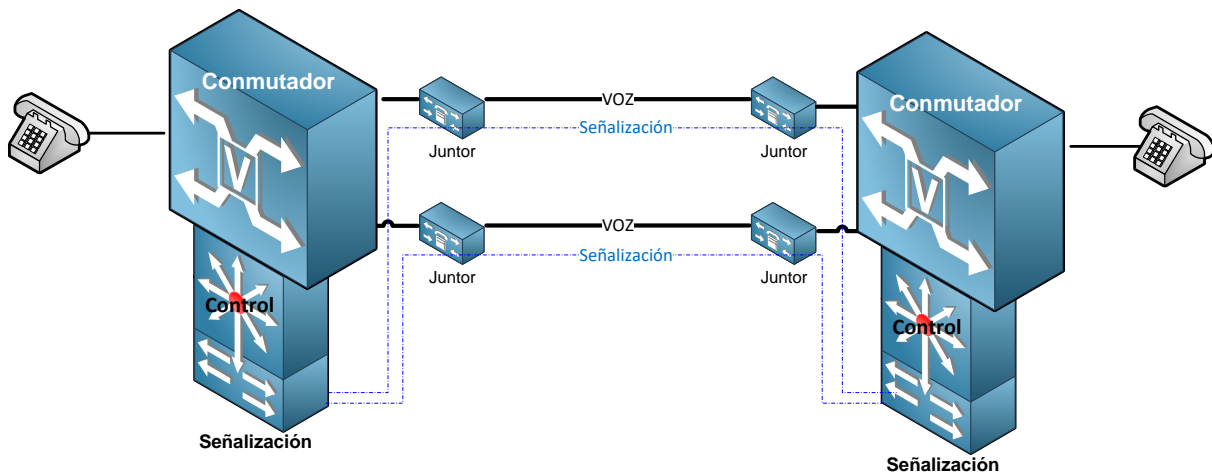


Figure A - 1. Channel Associated Signaling (CAS).

In CAS, the control plane information (e.g. routing) is encoded and transmitted in the same channel as the payload itself (e.g. voice). This introduces some limitations, namely:

- Inefficient resource/usage allocation
- Susceptibility to fraud
- Limited signaling states

### A.1.2.2 Common Channel Signaling (CCS)

As for ITU-T Q.9, a signaling technique in which signaling information relating to a multiplicity of circuits, and other information such as that used for network management, is conveyed over a single channel by addressed messages.

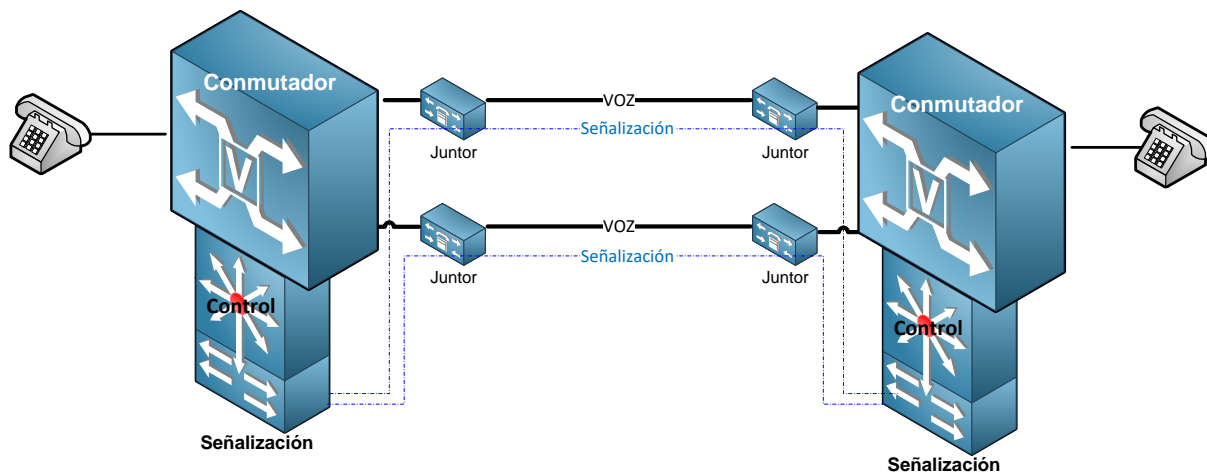


Figure A - 2. Common Channel Signaling (CCS).

One or more signaling channels transport control/routing information of all payload (voice/data) channels between service switching points. Signaling data is not rigidly assigned within the frame as in CAS or R2.

In CCS, control and user planes (signaling/data) are transmitted in separate channels. Thus, two physical networks, «speech» and «signaling» can have different paths. A single signaling channel controls multiple data channels, hence CCS improved efficiency in resource usage. Another advantage of CCS comprises its independence of transmission/switching technology.

CCS systems are packet-based, each signaling message is a block of information divided into fields according to recommendations and standards which define the structure of a message, including its fields and parameters. CSS operates in two distinct ways: Circuit and Non-Circuit Related Signaling.

Up to date, the only CCS systems implemented are Signaling Systems No. 6 and No. 7 (SS6 and SS7).

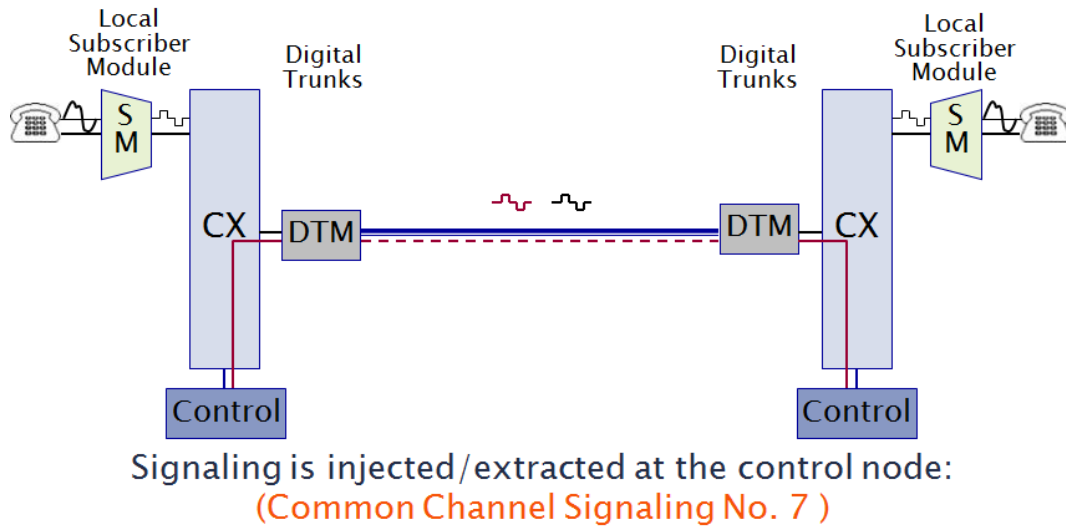


Figure A - 3. Common Channel Signaling path between signaling switching points.

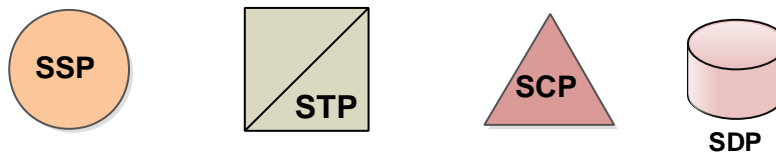
## A.2 Signaling System N°7 Network Entities

Each SS7 entity acts as a Signaling Point (SP), communicating each other through dedicated links. Three basic types of SPs exist in an SS7 network, namely:

- SSP (Service Switching Point)
- STP (Signaling Transfer Point)
- SCP (Service Control Point).

An SCP is commonly associated to at least one data base known as an SDP (Service Data Point). They are normally associated as the same network entity.

Geometric symbols like the ones exhibited next are typically assigned to the different SPs:



With the irruption of IN («Intelligent Networks»), besides complexity and capabilities increase at the SCP/SDP, other SPs rise, namely:

- IP (Intelligent Peripheral)
- SRF (Specialized Resource Function)
- SMP (Service Management Point)

Subscriber's lines connect to a telephony entity known as «Local Exchange» (LE), «Central Office» or «Class 5 Switch», which comprises the subscriber's entry point to the SS7 network. SSPs constitute switches that origin, bind and terminate calls. Besides, either for local or national planes, they offer specific services to subscribers such of those residing in certain intelligent network control nodes.



Figure A - 4. Service Switching Points control and user planes paths.

The purpose of a «Tandem Exchange» (TE), also known as «Class 4 Switch», is concentrating the traffic of several LEs and thus simplify routing throughout the network. Likewise, it can act as an SSP, as it can offer services to its incoming calls. This approach allows LE's SSPs indirectly communicate between each other, removing then the need of complex interconnection arrangements.



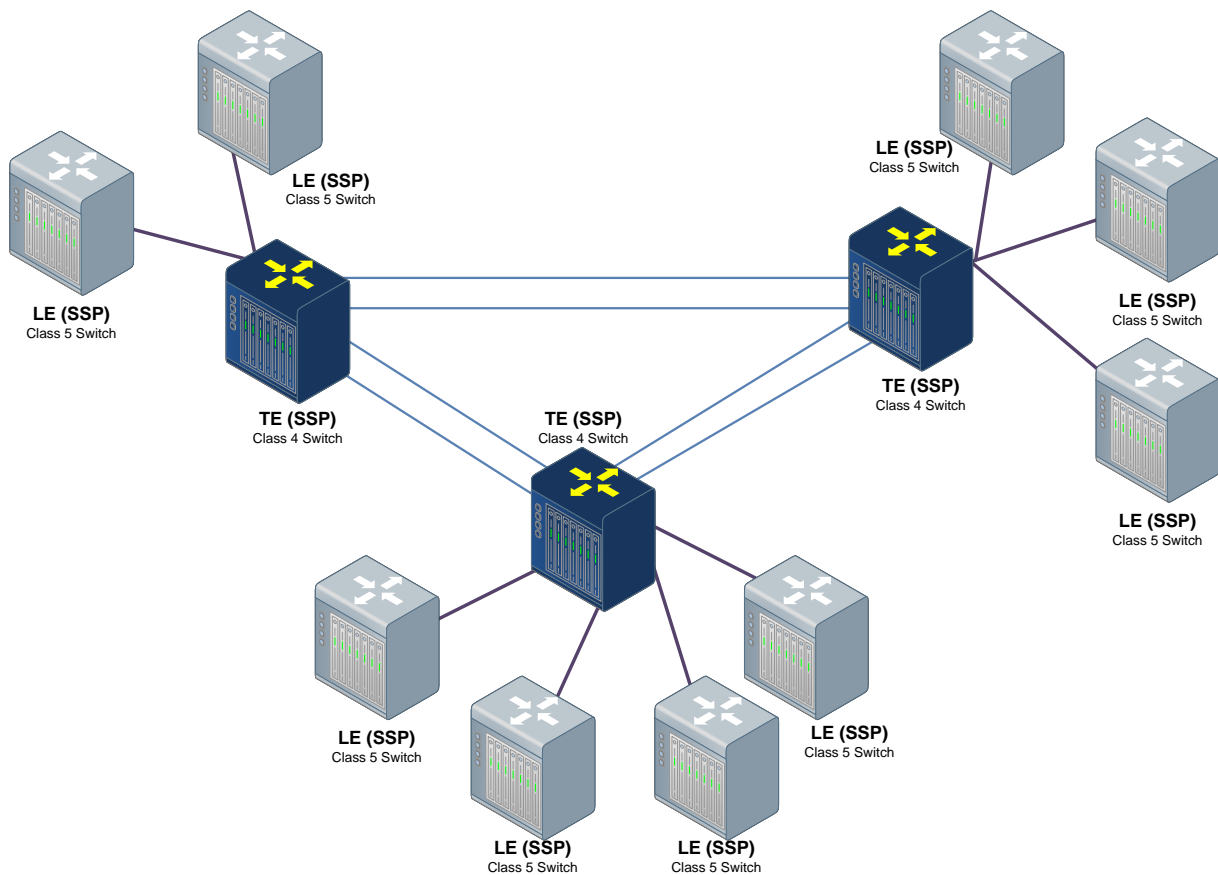


Figure A - 5. Network arrangement of Local and Tandem Exchanges.

A dedicated switch known as STP («Signaling Transfer Point») optimizes the use of the network, eliminating the need for direct links between different SPs. For the sake of redundancy, they are usually deployed in pairs. Likewise, an SP connected to an STP is also usually connected to its peer, so as to ensure routing resilience.

An STP comprises a signaling hub which only routes incoming messages towards the appropriate destination based on the embedded information. It does not offer service termination, as it typically does not deploy a user part.

As the network grows, the need for these types of networks architecture becomes more evident, so as to split different traffic types. The next diagram shows an example of how a network might be built to provide an efficient method of interconnecting unrelated switches while offering multiple routing possibilities. The

dotted lines represent some of the user plane transmission paths among subnetworks.

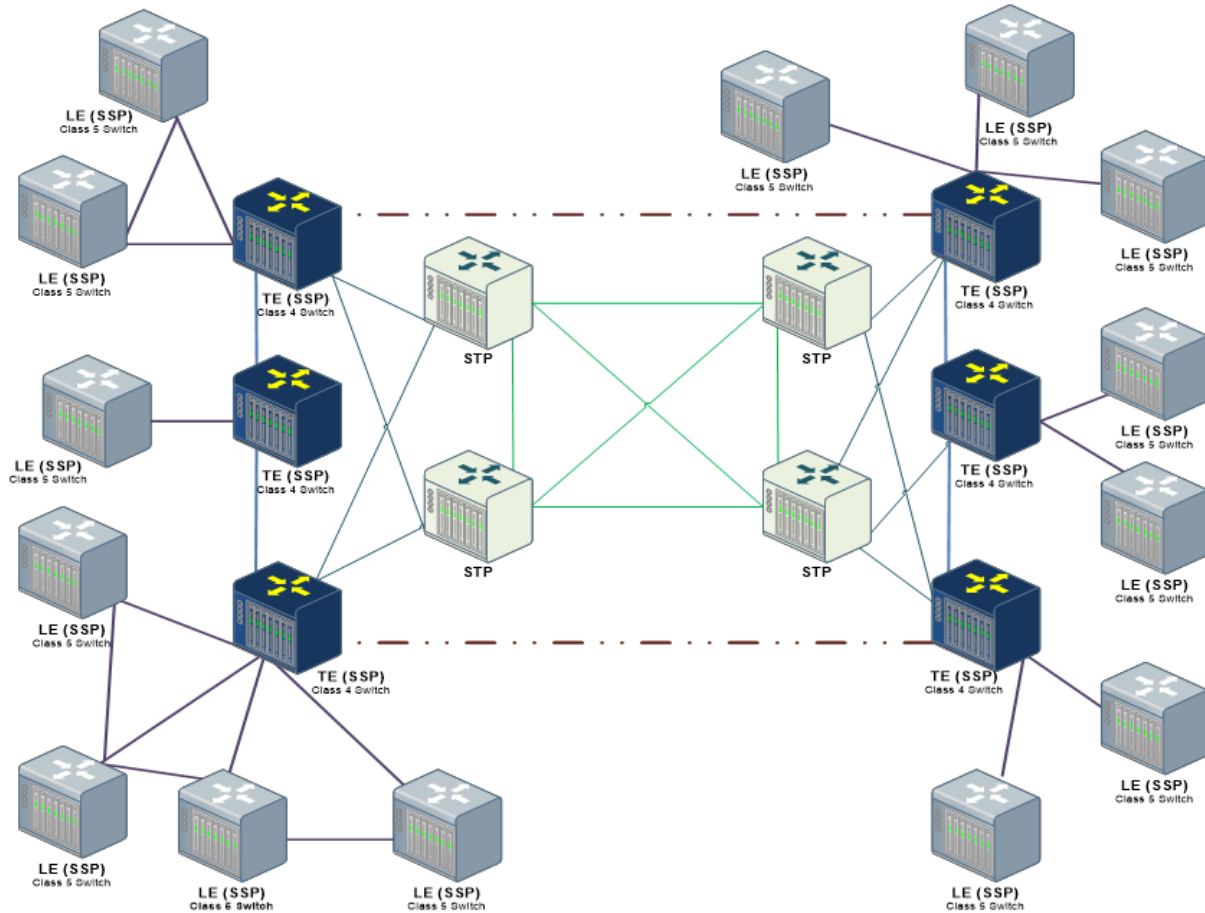


Figure A - 6. Network arrangement of STPs and SSPs.

An SCP comprises a control node within the SS7 network. It allows access from every signaling point of the network to services implemented in specific entities via special signaling messages, constituent of the Intelligent Network concept or IN.

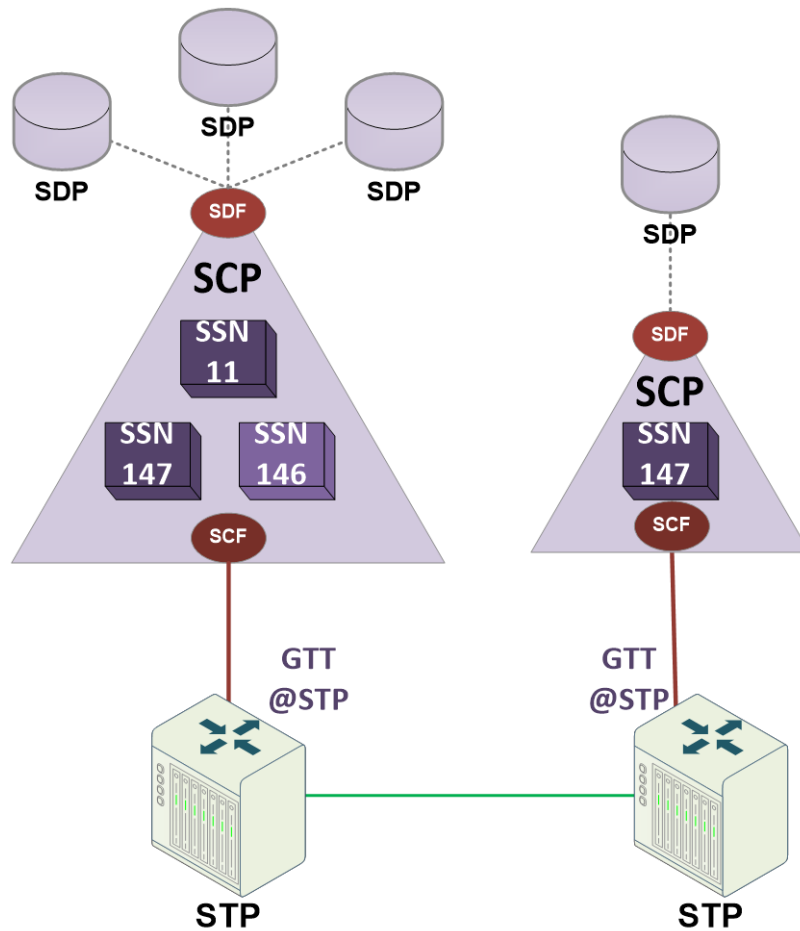


Figure A - 7. SCP's connections to STPs for GTT.

The IN defines a series of standards which allow cost-effective addition of new services and almost none interference with existing networks. An Intelligent Network splits the logic from the control plane and concentrates services in dedicated network resources.

The SPs (SSPs, STPs, etc.) communicate with SCPs through a special set of signaling messages as the ones defined by the INAP or the CAP protocol (either for fixed or mobile networks correspondingly).

The SCP provides the service logic via the Service Control Function (SCF), which processes the IN service. It also provides user and/or network information via the Service Data Function (SDF).

The SSP brings access to IN capabilities. An SSP usually comprises switching functions called Call Control Function (CCF) and Service Switching Function (SSF) which provide interaction with the SCP.

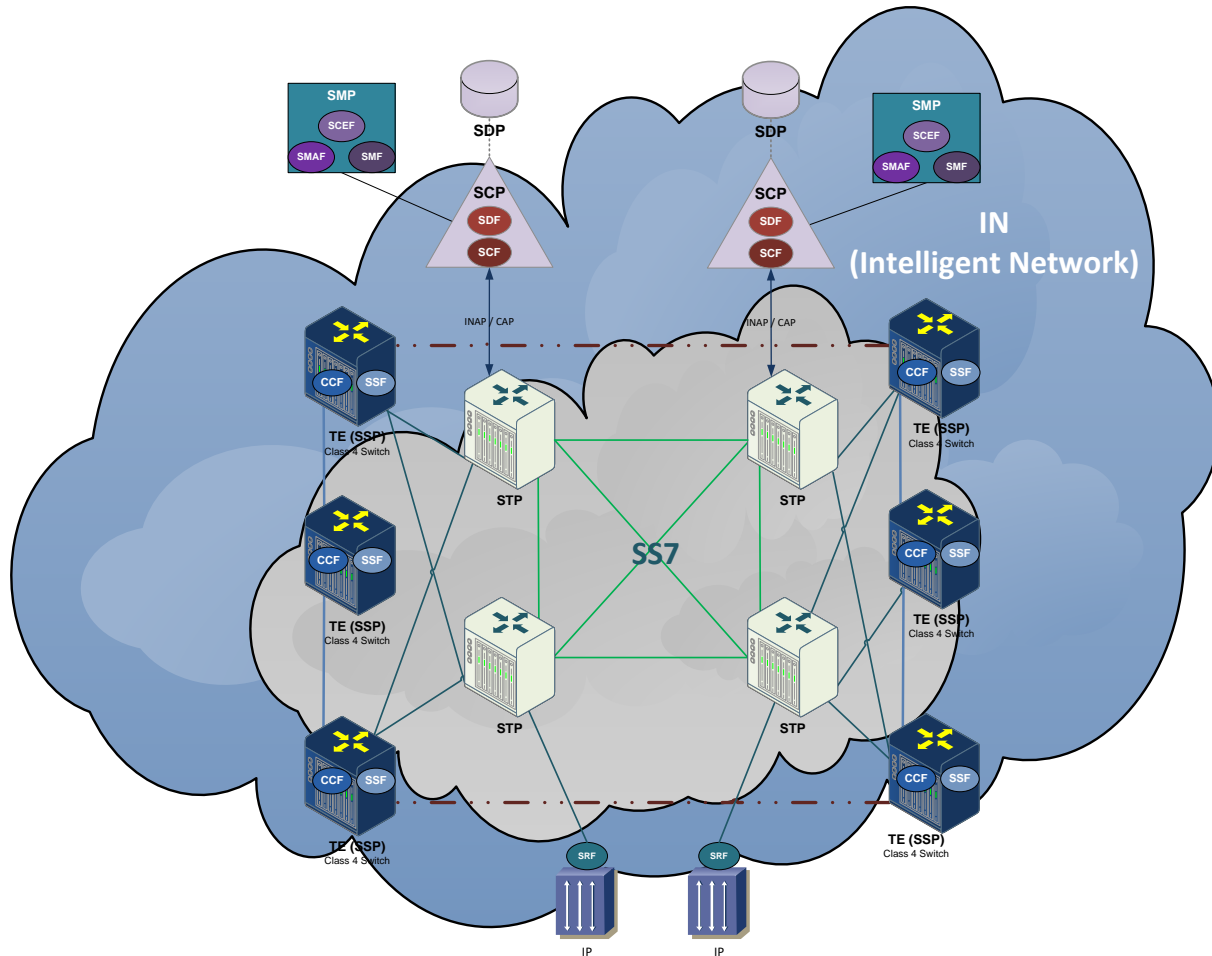


Figure A - 8. Intelligent Network entities internetworking.

The Intelligent Peripheral (IP) provides the special resources needed for the support of IN services through the Specialized Resource Function (SRF), e.g, voice announcement, DTMF collect digits, automatic speech recognition, audio conference bridge, protocol translation, etc.

The Service Management Point (SMP) performs management tasks like service control management, service provisioning, data base administration, new service testing, special user selection, etc.

Each new IN service can be quickly added as they only affect the SCPs and IPs, but not the rest of signaling entities.

IN services are mostly initiated by triggers. An SSP can detect when a service is invoked by correlating its triggers within its routing tables. For example, when an IN service invoke is detected in a call, the SSP will retain it and transfer control to the SCP by IN signaling. The SCP will refer its data base (SDP) so as to recognize the calling part as well as the profile of the activated service. Once every need is identified for the IN service, the SCP can negotiate with the SSP for providing information concerning to the new call destination and make further requests of voice connection resources, so that it can send instructions to the user.

## A.2.1 Signaling Modes

### A.2.1.1 Associated Signaling Mode

In associated signaling mode, either the channels carrying signaling data or those carrying user payload (speech/data) follow the same direct path between adjacent signaling points.

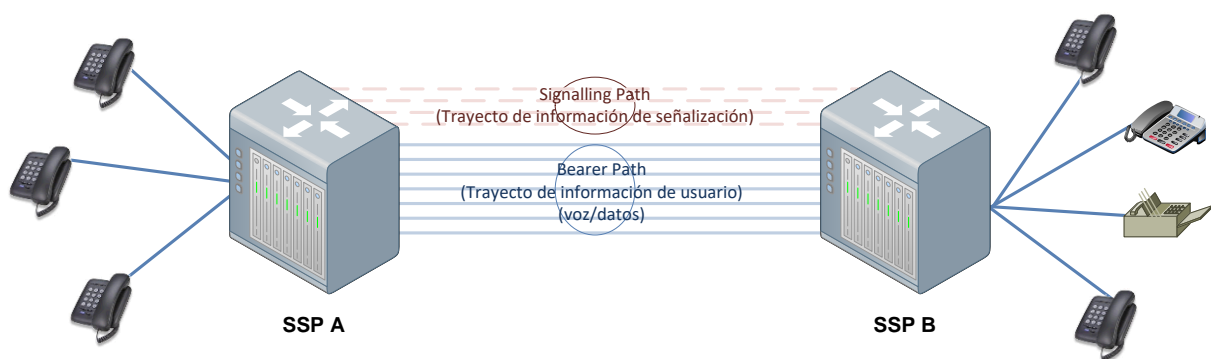


Figure A - 9. Associated Signaling Mode.

### A.2.1.2 Non-Associated Signaling Mode

In non-associated signaling mode, the signaling data is routed between non-adjacent or distant signaling points through an undetermined path via two or more intermediary STPs.

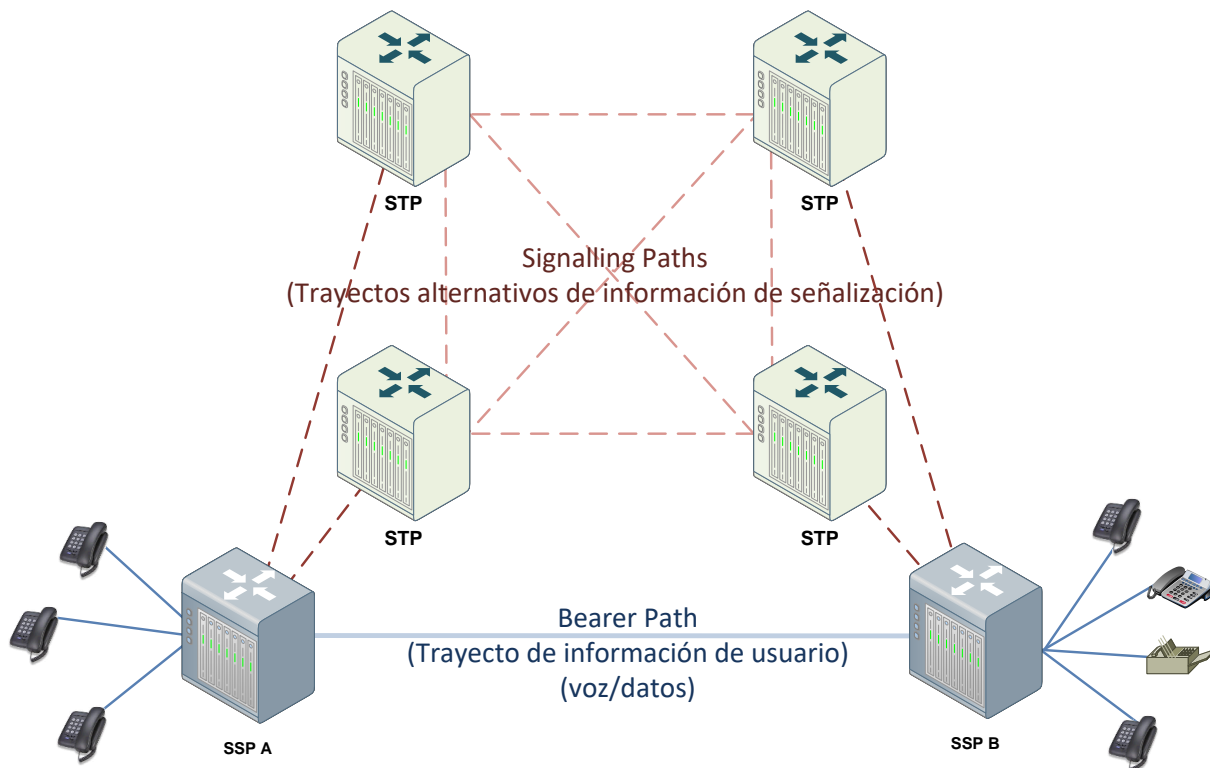


Figure A - 10. Non-Associated Signaling Mode.

### A.2.1.3 Quasi-Associated Signaling Mode

In quasi-associated signaling mode, the signaling information is routed between two non-adjacent or distant signaling points, connected to the same pair of STP nodes through a predetermined route.

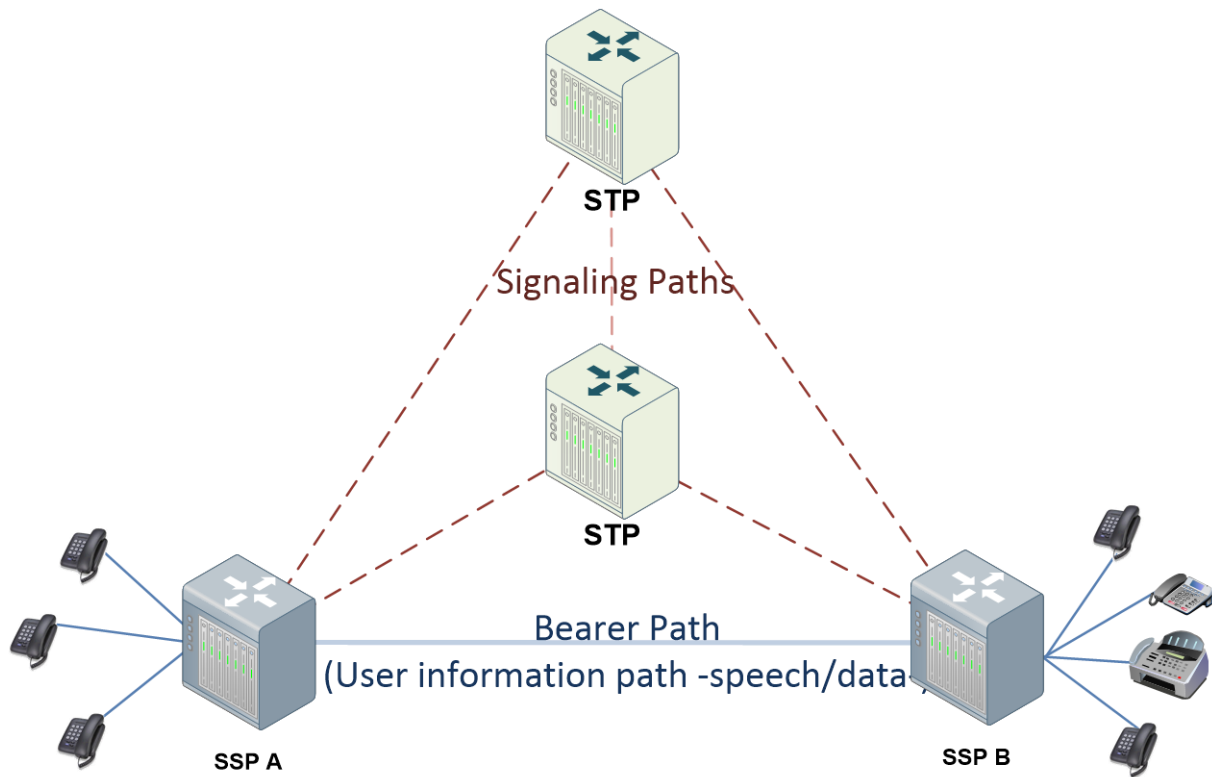


Figure A - 11. Quasi Associated Signaling Mode.

### A.2.2 Links and Linksets

Links connect neighbour network entities establishing communication routes between them.

Each SP within the network is identified by a unique address named SPC (Signaling Point Code). Each SS7 message has an Originating Point Code (OPC) and a Destination Point Code (DPC). The SPC comprises a finite series of bits, hence, there is a finite amount of SPCs within a national or international network.

Links are usually grouped in linksets. A linkset is a cluster of links sharing the same destination and, although non-mandatory, usually established directly between the same SPs. The message load in a linkset is typically shared between the active links, being this part of the inherent robustness of the SS7 stack, as the links of a

linkset are redundant. Hence, the load of a linkset is conveyed and shared among the active links during link failures. Up to 16 links can be established between two SPs.

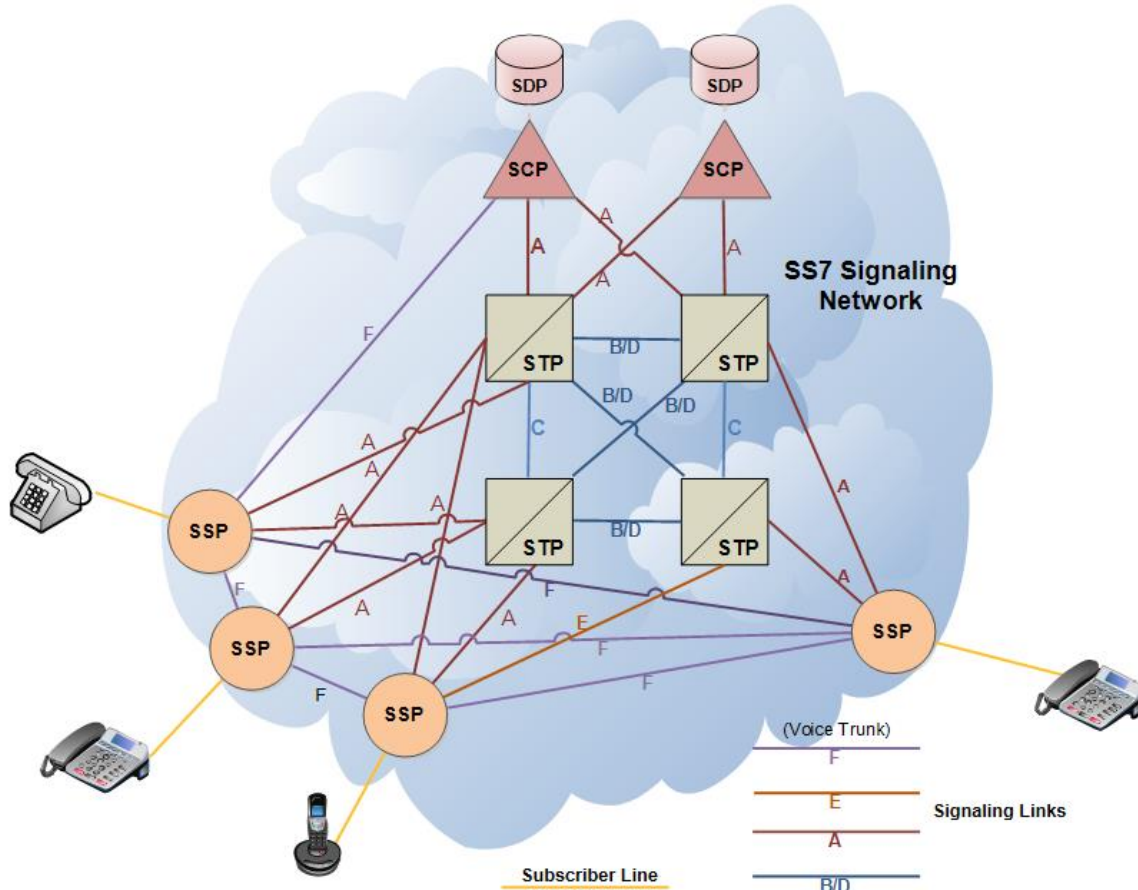


Figure A - 12. Type of signaling links in SS7.

Link Type	Description
A	An <b>Access</b> link connects a signaling end point or source point (e.g. SCPs or SSPs) to an STP. Only messages originating from or destined to the signaling end point are transmitted on an "A" link.
B	A <b>Bridge</b> link connects STPs. Typically, quads of B links interconnect primary STPs of one network to primary STPs of another network. The distinction between B and D links is rather arbitrary (hence, such links may be referred to as B/D links).
C	<b>Cross</b> link connects STPs performing identical functions into a mated pair; they are used to improve the reliability of the signaling network. A C link is only



	used when an STP has no other route available to a destination signaling point due to link failures. SCPs may be deployed in pairs for redundancy. Yet, signaling links do not interconnect mated SCPs.
D	A <b>Diagonal</b> link connects pairs of STPs at different hierarchical levels (e.g. a secondary either local or regional STP pair to a primary internetwork gateway STP pair in a quad-link configuration). Secondary STPs within the same network are connected via a quad of D links.
E	An <b>Extended</b> link connects an SSP to an alternate STP to provide an alternate signaling path. E links are not usually provisioned unless the benefit of a marginally higher degree of reliability justifies the added expense.
F	A <b>Fully</b> associated link connects two signaling end points (for example., SSPs and SCPs). F links are not usually deployed in networks with STPs, because they bypass the security features provided by the STPs. In networks without STPs, F links directly connect signaling points.

Table A - 1. SS7 link types.

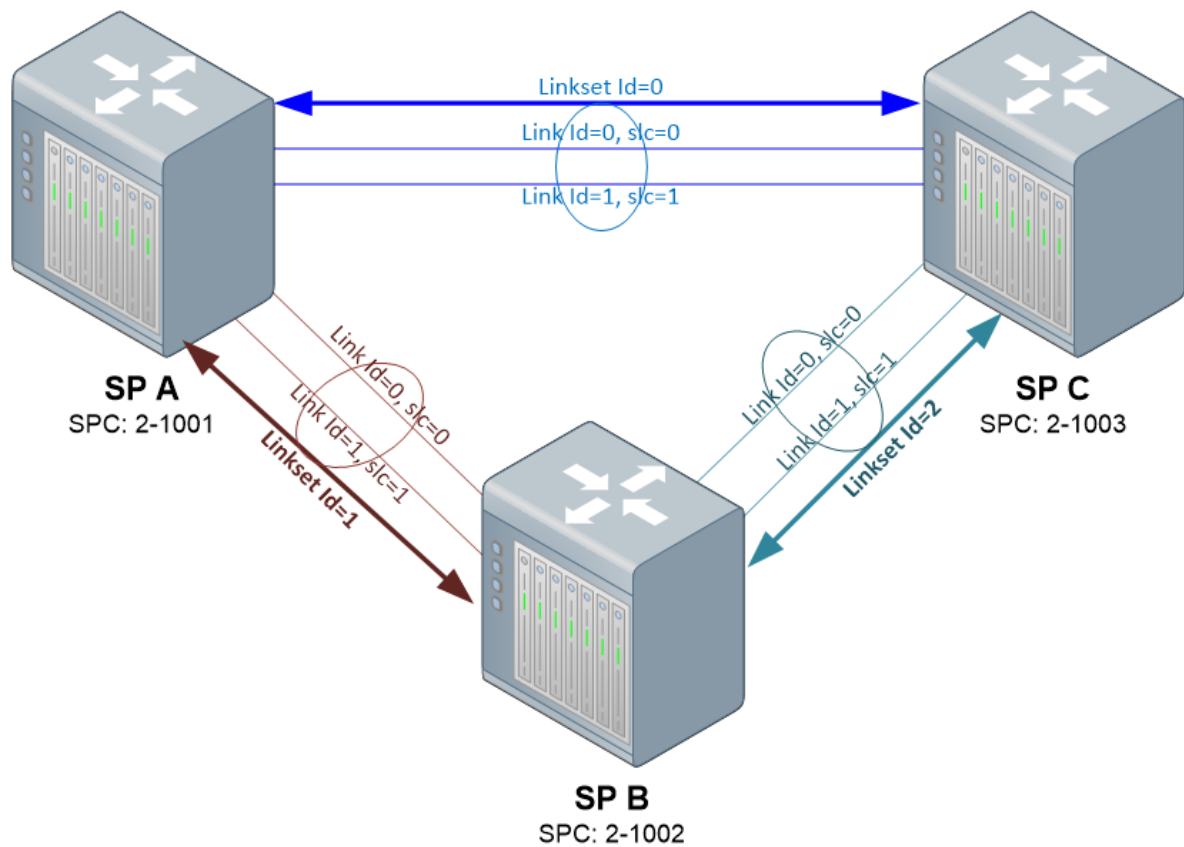


Figure A - 13. Link and linkset arrange between three SPs.

### A.2.3 Route and Routesets

A route is established whenever two SPs are communicated between each other. In other words, a route is the existing path between two SPs. A route may include one or multiples linksets. SPs may route messages to other SPs not directly connected between each other. In these cases, the route describes the path taken by the network between ends. Whenever alternative paths exist between two SPs, collection of routes known as Routeset is present.

In SS7 signaling, the link constitutes the fundamental unit. Links are grouped in Linksets, which in turn shape Routesets. Alike the links of a linkset work together to assure information transmission, the possibility of supporting alternate routes towards the same destination enhances the network robustness.

SS7 may then be understood within the context of information transport throughout the network via the most convenient path.

Regarding the previous diagram of Figure A-13, adding an additional network node is observed in next one in Figure A-14, so that for example, the potential paths between B and D, have increased significantly. B possesses 3 routes towards C and 4 routes towards D, handling then 2 routesets with 3 and 4 routes respectively.

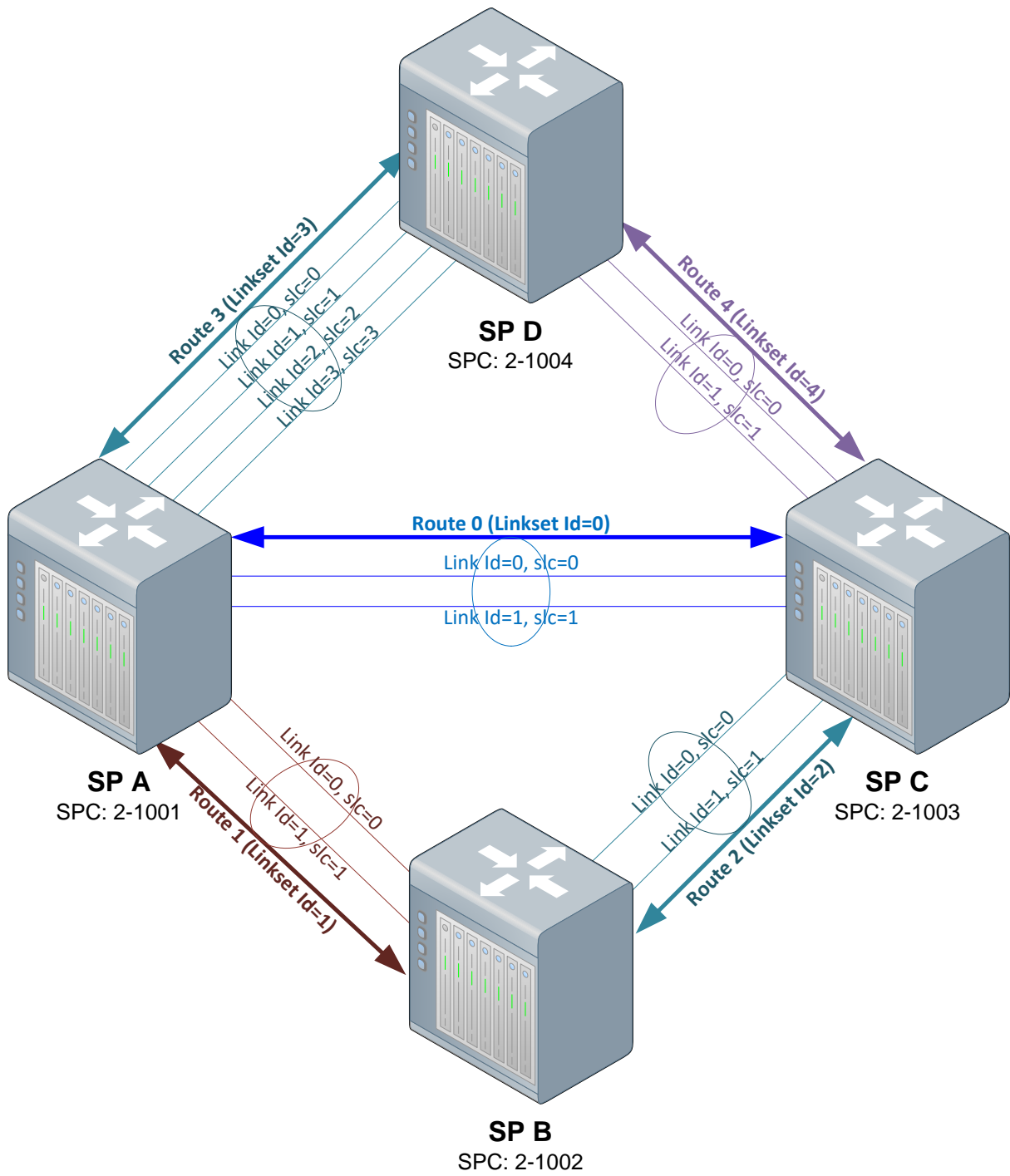


Figure A - 14. Route and routesets and their respective linksets between four SPs.

## A.3 SS7 Protocol Stack

SS7 comprises a suite or stack of protocols which use a common transport mechanism for the distribution of several messages among the network entities.

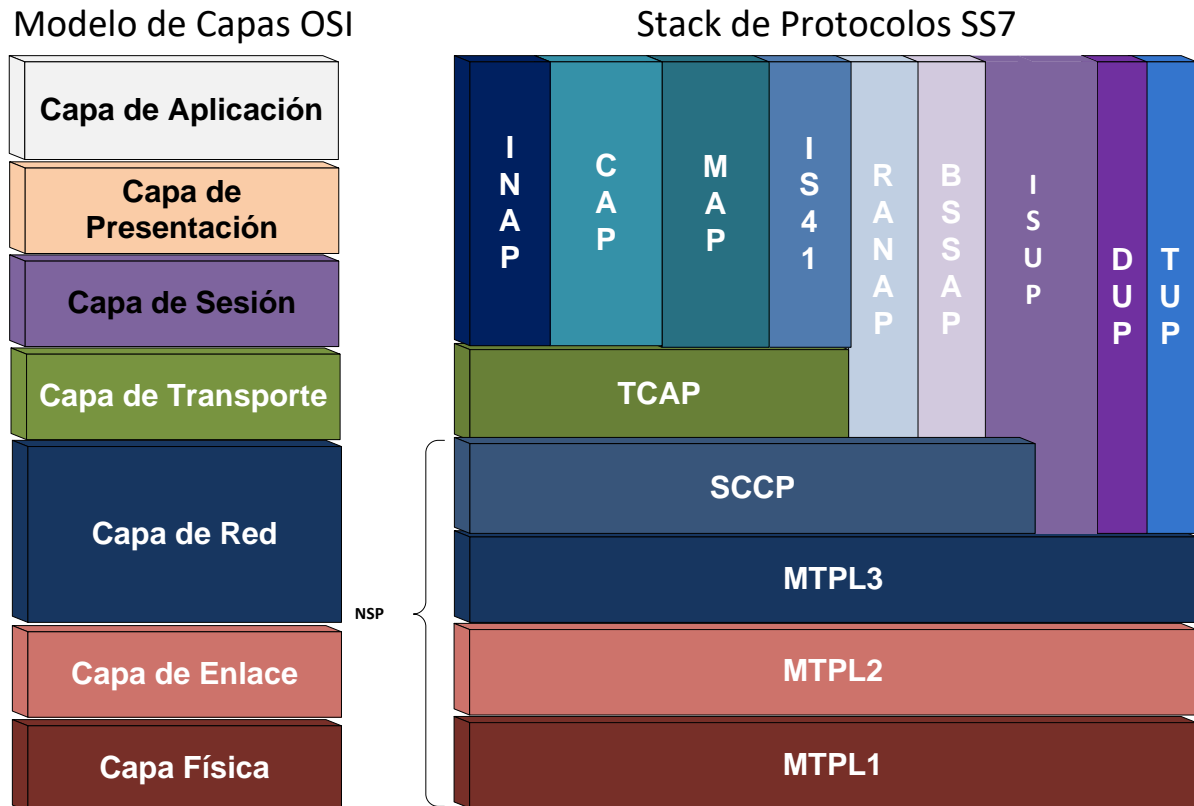


Figure A - 15 SS7 Protocol Stack versus OSI Layer Model.

SS7 comprises a hierarchical structure in layers, similar but not exactly correspondent with the OSI reference model as shown in Figure A-15.

### A.3.1 Message Transfer Part (MTP)

The three lowest level layers of the SS7 stack are grouped in the Message Transfer Part (MTP), defined by ITU-T Recommendations Q.701 to Q.709.

MTP layer is responsible for reliable routing of messages and link management among the SS7 network. It is divided in 3 layers functionally discriminated for executing specific functions.

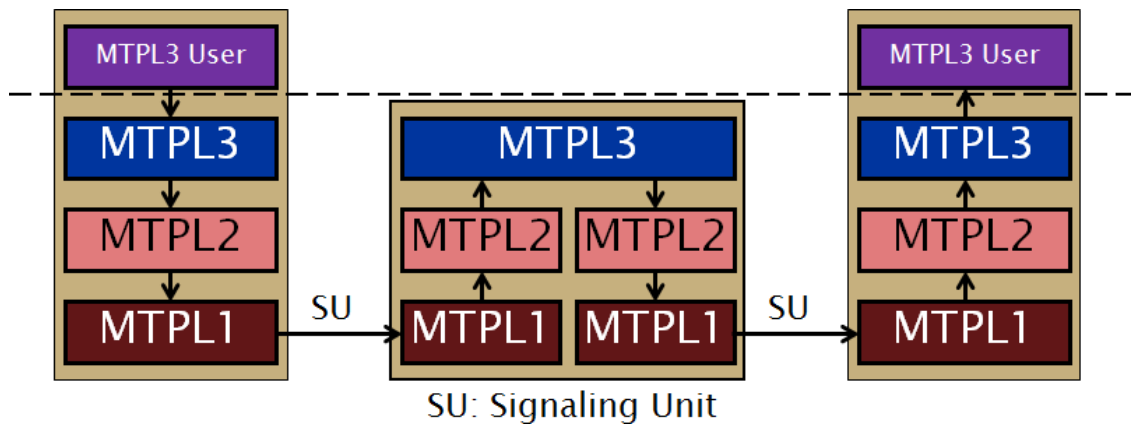


Figure A - 16. Signaling Unit path between MTP users.

### A.3.1.1 MTP Layer 1: Signaling Data Physical Layer

MTPL1 defines the physical, electrical, and functional characteristics of a digital signaling link and the means for its access. Defined physical interfaces include: E1 (2.048 Mbps), DS1/T1 (1.544 Mbps), V.35 (64 kbps), DS0 (64 kbps), and DS0A (56 kbps).

It is mainly responsible for the following:

- Connection of adjacent SS7 SPs within the transmission network.
- Digital message to electrical signals codification/decodification.
- Maintenance of physical links.

For economy reasons, digital transmission networks are shared by data/voice and signaling links:

- Some PCM systems only transport voice/data channels.
- Other systems also carry signaling channels.

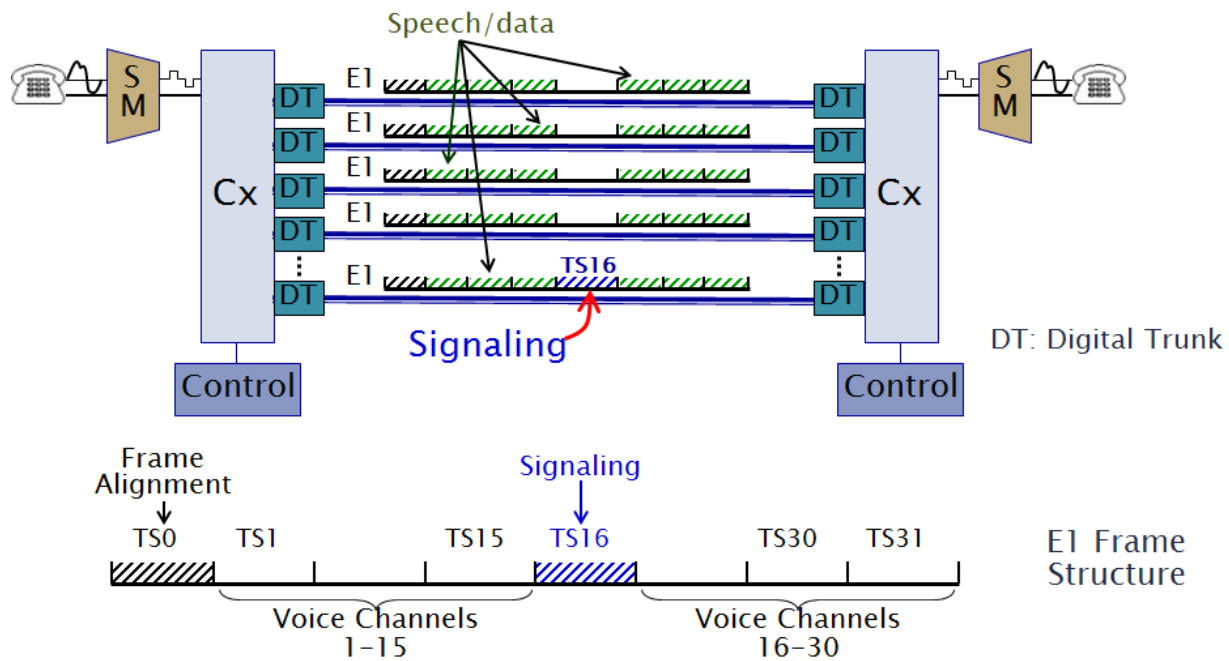


Figure A - 17. Signaling data links and E1 frame structure.

An E1's (2.048 Kbps) Time Slot 16 (TS16) transports signaling information of several E1s.

### A.3.1.2 MTP Layer 2: Signaling Link Layer

Based on the HDLC (High-Level Data Link Control) protocol, MTP2 defines the needed functions and procedures for the reliable transfer of signaling messages between adjacent SPs through a determined signaling link between them, namely:

- Signaling unit allocation: flags → assemble of known packets known as signaling units: FSSU/LSSU/MSU.
- Ambiguity prevention (flag imitation): filling bits.
- Error detection: Cyclic Redundancy Check (CRC)
- Error correction: retransmission and sequence control.
- Signaling link failure detection: error rate supervision.
- Signaling link alignment: Initial synchronicity or recovery.

### A.3.1.2.1 Signaling Units

MTPL2 is designed to provide reliable transfer of signaling information between SPs, which involves among other functions, assembly of packets known as Signaling Units, three SUs are defined, namely:

- *Fill In Signaling Unit (FISU)*: packet transmitted continuously on a signaling link in both directions to keep the link alive and aligned when no other SU traffic is present;
- *Link Status Unit (LSSU)*: link status information exchange packets;
- *Message Signaling Unit (MSU)*: upper SS7 layers message container.

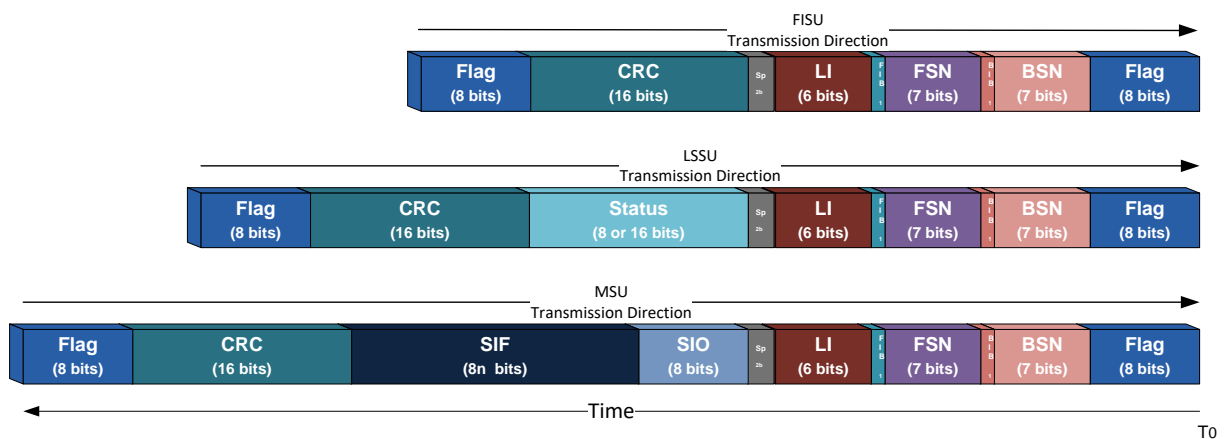


Figure A - 18. SS7 Signaling Units.

#### A.3.1.2.1.1 Message Signal Unit (MSU)

MSUs are used for transporting messages of upper layers embedded in MTPL3 (TUP, DUP, ISUP, SCCP, etc.). It contains the following fields:

- **Flag:** Frame boundary: 01111110. For avoiding flag imitation, filling bits are used:
  - Away from flags within a SU, after five consecutive “1”, the transmitter entity inserts a “0”.
  - The receiving entity, post flag recognition, it eliminates every “0” appearing after five consecutive “1”.

- **BSN**: Backward Sequence Number. It consists of the sequence number of the last correctly received MSU (receipt acknowledgement).
- **FSN**: Forward Sequence Number. Flag bit which indicates if a remote end status change has occurred and requests a retransmission of the message, if it has been received out of sequence
- **BIB**: Backward Indicator Bit. It consists of the MSU's direct transmission sequence number.
- **FIB**: Forward Indicator Bit. Flag bit that indicates the start of a retransmission cycle.
- **LI**: Length Indicator (for MSUs it takes values in the 3-63 range);
- **SIO**: Service Information Octet;
- **SIF**: Signaling Information Field. It can spread between 2 and 272 octets.
- **CRC**: Cyclic Redundancy Check. Error detection code used to detect accidental data deviations. The receiving terminal obtains the code and compares with the received bits. If there is a mismatch, it discards the SU

#### **A.3.1.2.1.2 Fill In Signal Unit (FISU)**

Used in idle periods, when there is no information to send, in order to keep alignment. In FISU, LI field takes the value «0».

#### **A.3.1.2.1.3 Link Status Unit**

Transport of minimum information for signaling link state supervision at the remote end (e.g. alignment). In FISU, LI field takes the value «0» or «1».



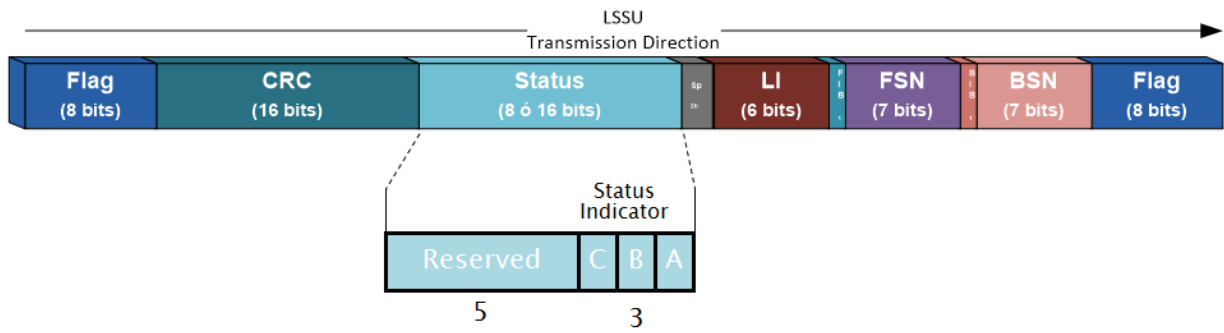


Figure A - 19. LSSU structure.

C	B	A	Status Indicator
0	0	0	<b>SIO:</b> Status Indication "O" ("out of alignment")
0	0	1	<b>SIN:</b> Status Indication "N" ("normal alignment")
0	1	0	<b>SIE:</b> Status Indication "E" ("emergency alignment")
0	1	1	<b>SIOS:</b> Status Indication "OS" ("out of service")
1	0	0	<b>SIPO:</b> Status Indication "PO" ("processor outage")
1	0	1	Status Indication "O" ("out of alignment")

Table A - 2. Status Indicator possible values description.

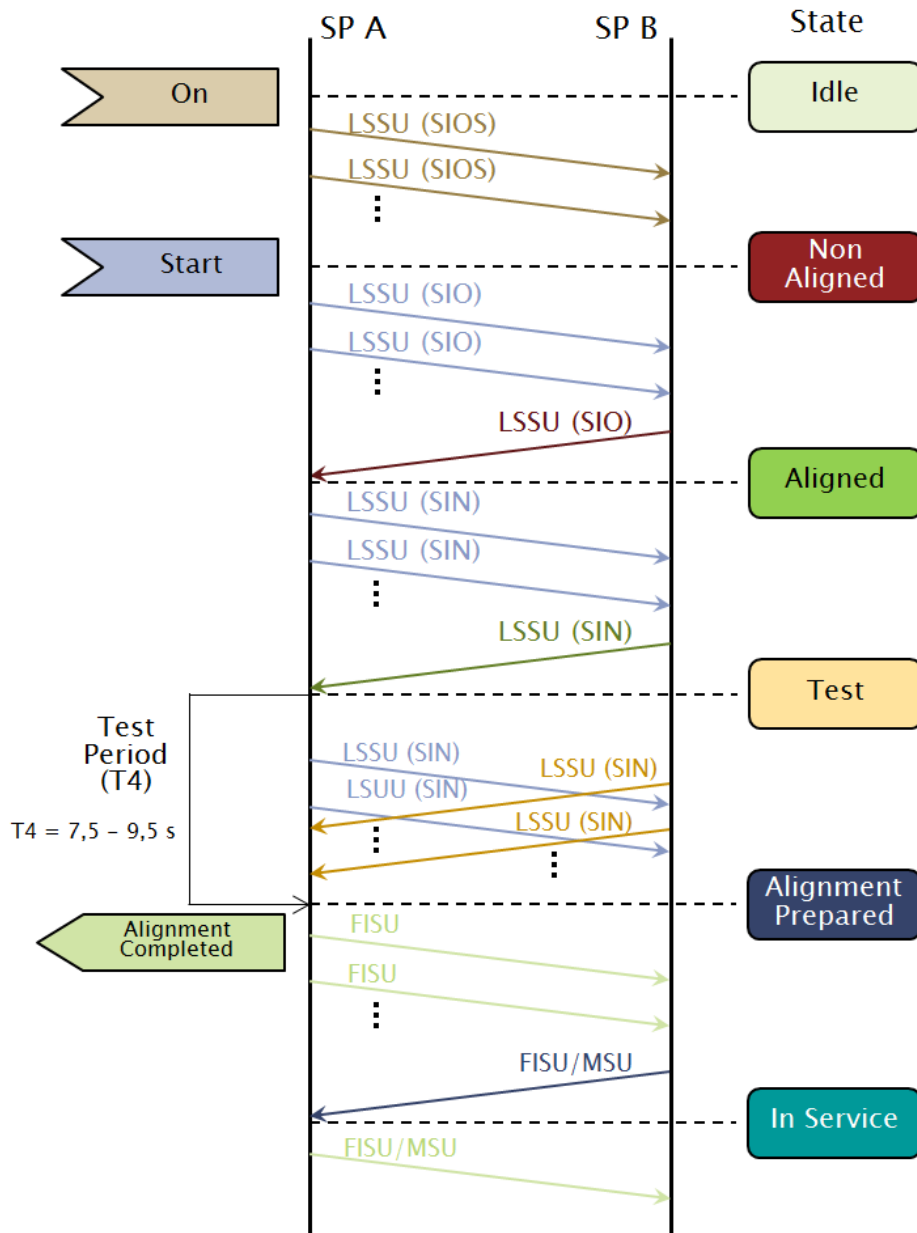


Figure A - 20. LSSU message exchange for initial link alignment

#### A.3.1.2.1.4 Error Correction

MTPL2 uses two methods for error correction:

- *Basic method*: used when the transmission delay in one direction of the signaling link is shorter than 15.

- *Preventive cyclic retransmission method*: used when the transmission delay in one direction of the signaling link is bigger than 15 (satellite or intercontinental links).

In the basic method, receiver returns positive acknowledgements (correct reception) and negative acknowledgements (error). On positive acknowledgement, next MSU contains:

- ✓ BSN = FSN of the received MSU.
- ✓ BIB = FIB of the received MSU.

On negative acknowledgement, next MSU contains:

- ✓ BSN = FSN of the last correctly received MSU.
- ✓ BIB = FIB of the last correctly received MSU, inverted.

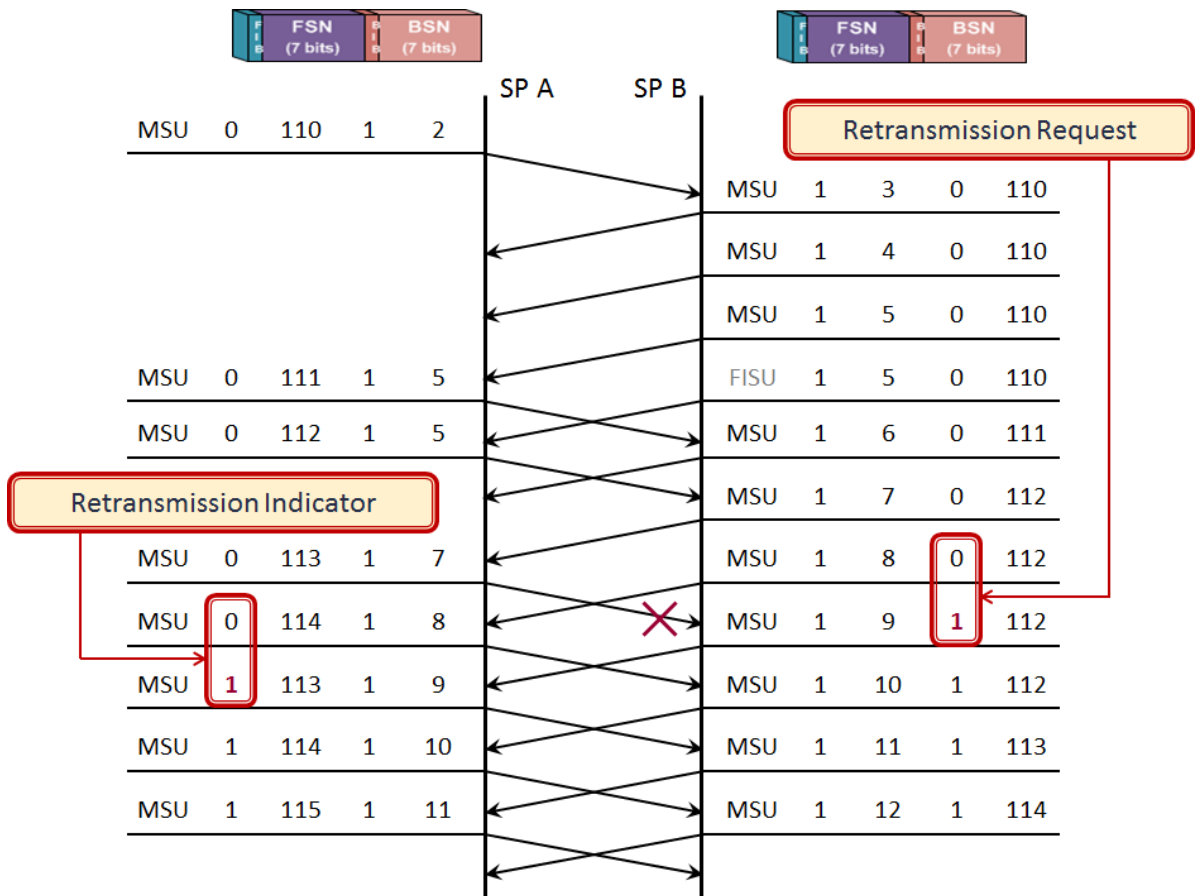


Figure A - 21. Example of message exchange according to the MSU basic error control method in MTPL2.

In preventive cyclic retransmission error correction method, the following rules apply:

- No negative acknowledgements.
- When no new MSUs exist, buffered MSUs are cyclically transmitted.
- New MSUs have highest priority.
- MSUs receiving positive acknowledgement are flushed from the retransmission buffer.
- In case of high signaling traffic load (high number of new MSUs), forced retransmission is carried out.

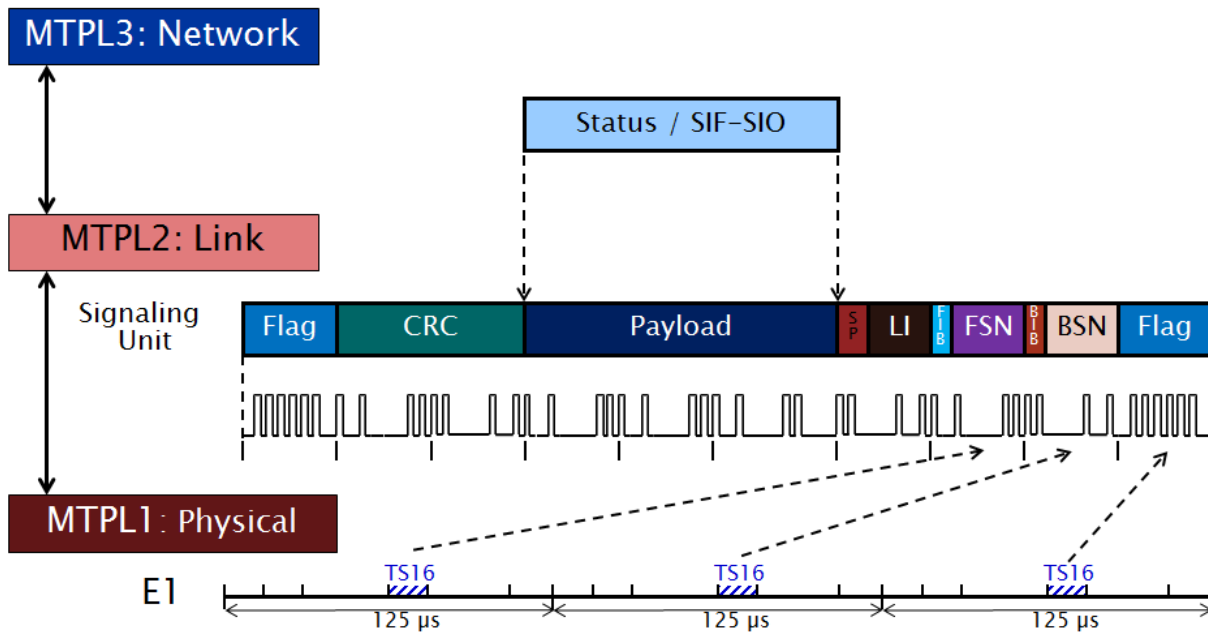


Figure A - 22. Signaling Unit Assembly.

### A.3.1.3 MTP Layer 3: Signaling Network Layer

MTPL3 provides signaling message transport functions and procedures, routing and management/congestion control of the signaling network, independent of individual signaling links.

ITU-T defines 14 bits SPC, meanwhile ANSI uses 24 bits (3 octets). This fact evidences the need of routing information throughout ANSI and ITU-T networks by an STP which interprets both variants and is able to establish a communication.

SPCs according to ITU-T are composed of pure binary numbers which might be established in terms of zone, area/network and point code identifiers.

SPC according to ANSI are composed by the octets Network, Cluster and Member (e.g.: 242-16-0).

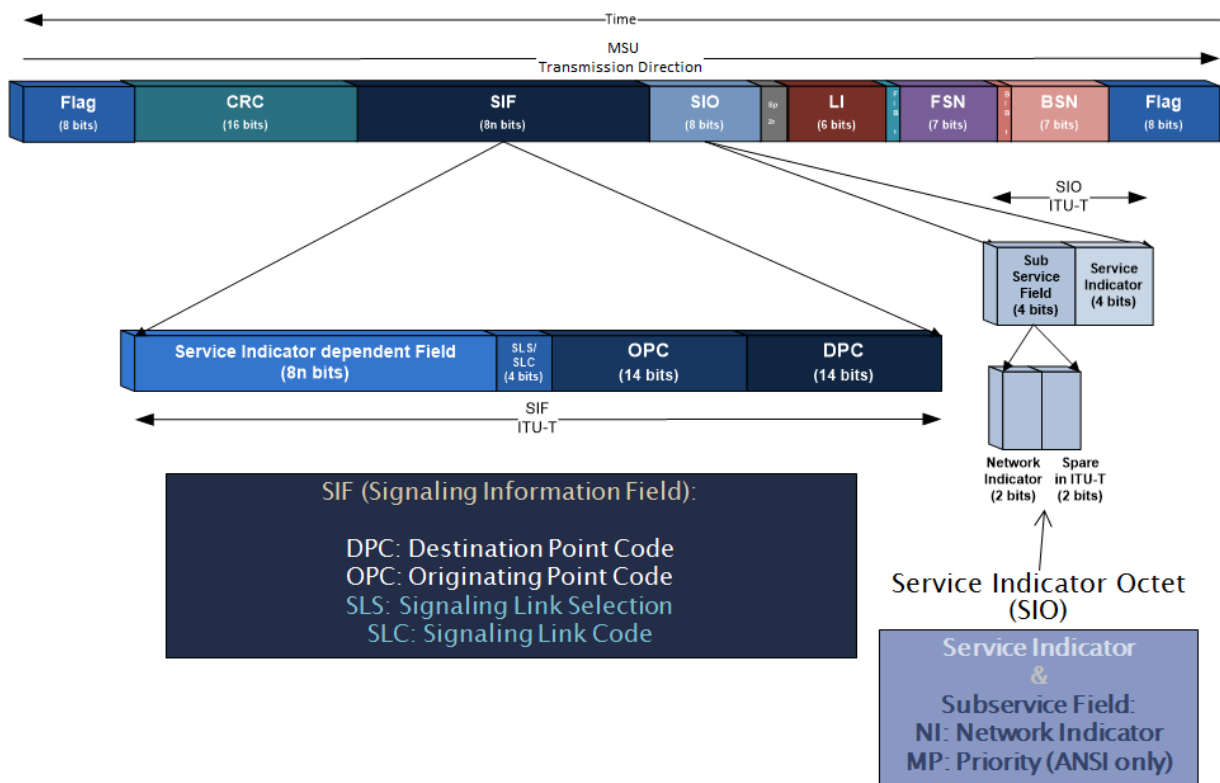


Figure A - 23. MSU: Routing Label and Service Indicator Octet (ITU-T).

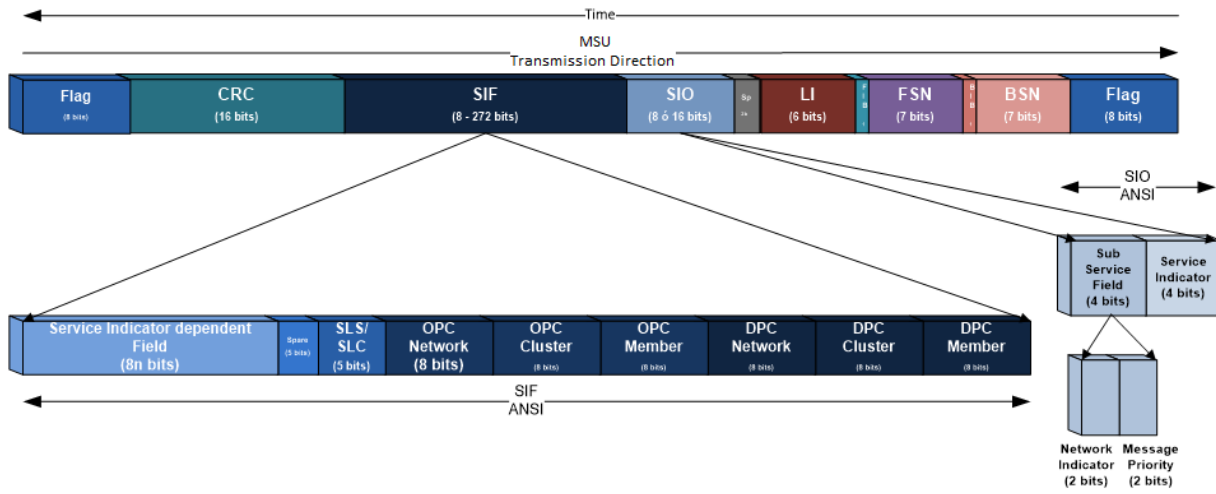


Figure A - 24. MSU: Routing Label and Service Indicator Octet (ANSI).

**A.3.1.3.1 MTPL3 Treatment of Signaling Messages functions**

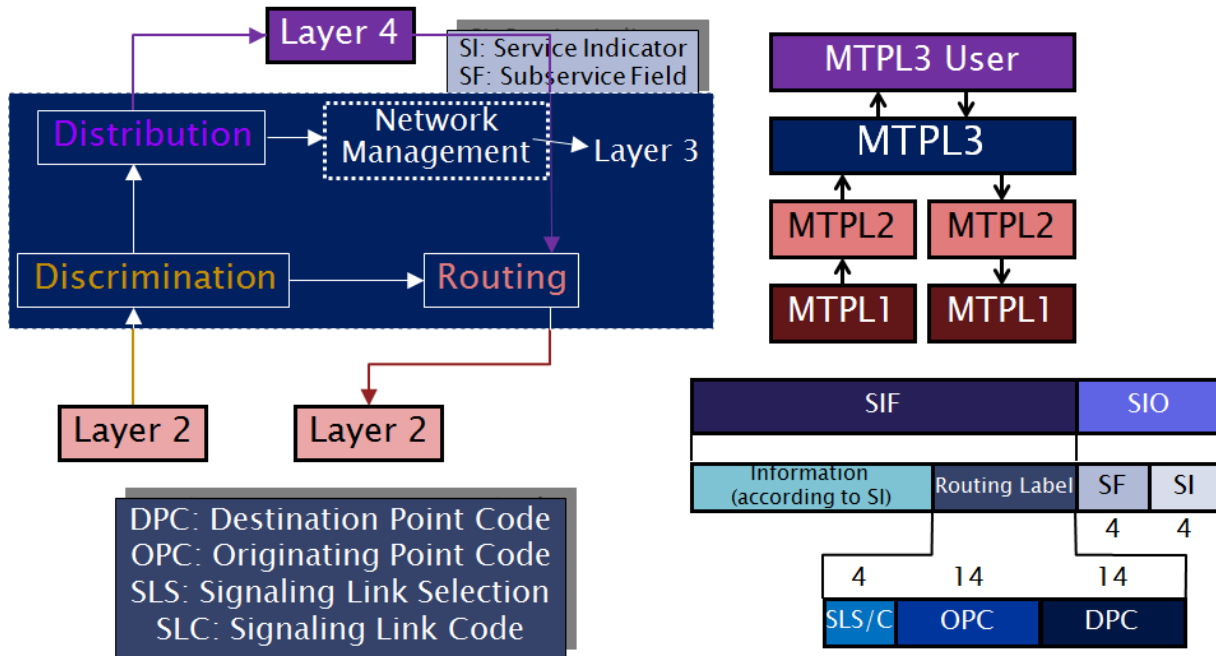


Figure A - 25. MTPL3 treatment of signaling messages functions.

*Treatment of Signaling Messages functions* involve routing of messages to the appropriate destinations of any of the SS7 stack layers (user part of the destination signaling point), namely:

- *Discrimination*: determines if the message is conveyed to other signaling point or towards itself.
- *Distribution*: sends the message either to layer 3 or 4, depending on the Service Indicator (SI in SIO).
- *Routing*: choosing of the signaling link to which the message is being sent.

#### **A.3.1.3.1.1.1 Routing Label (ITU-T)**

The routing label is the key component of MTPL3 routing functions. According to ITU-T, the routing label is composed of the following fields:

- **OPC/DPC (Originating/Destination Point Code)**: Each signaling point has its own identification. It works like an address within the signaling network at this level (MTP). ITU-T established a numeration plan in two independent levels: international and national. An International transit exchange SP must have two codes, one for each network. The international signaling point codes are managed by the ITU-T. The national signaling point codes are managed by the local national regulatory entity. While international SPCs discriminate zone (continent), area/network and signaling point, national signaling point codes categorize region, zone and signaling point.
- **SLS (Signaling Link Selection)**: Determines the particular signaling link to be used if more than one link is used for signaling (load sharing), and being the case, it also determines the group of links or linkset to use in the transfer of Layer 4 (e.g.: ISUP, SCCP).
- **SLC (Signaling Link Code)**: Replaces the SLS when the message corresponds to Layer 3 (e.g.: SNM, MTN/S, MTP), so as to indicate to which signaling link the message belongs. In other words, for MTP management information, the signaling link code (SLC) is used to indicate the signaling route.

### A.3.1.3.1.1.2 Service Information Octet

The Service Information Octet (SIO) field of an MSU is the key component of MTPL3 distribution functions. SIO is designed for packet discernment and is divided in two fields of 4 bits:

- Sub-Service Field: contains two sub-fields:
  - Network Indicator: International Network (0), Reserved only for international use (1), National Network (2) and Reserved only for national use (3). For the case of an international transit exchange, it determines if the SPC corresponds to the international or the national network.
  - Message priority (ANSI only, not used in ITU-T).
- Service Indicator: refers to possible layer 4 protocol, discriminated according to a particular value as depicted in next table.

SI (Service Indicator)		MTPL3 User
Binary	Hexadecimal	
0000	0	Signaling Network Management Message (SNM)
0001	1	Maintenance Regular Message (MTN)
0010	2	Maintenance Special Message (MTNS)
0011	3	Signaling Connection Control Part (SCCP)
0100	4	Telephone User Part (TUP)
0101	5	ISDN User Part (ISUP)
0110	6	Data User Part (DUP call and circuit-related messages)
0111	7	Data User Part (DUP facility registration/cancellation messages)
1000	8	Message Transfer Part (MTP reserved)
1001	9	Broad Band ISDN User Part (Broad Band ISUP)
1010	A	Satellite ISDN User Part (Satellite ISUP)
1011-1111	B-F	Reserved

Table A - 3. MTPL3 user according to Service Indicator value.



**A.3.1.3.2 MTPL3 Network Management of the Signaling Network functions**

*Network Management of the Signaling Network* functions involve routing traffic control, load sharing between the signaling links and error management.

- *Signaling Link Management*: controls the local links and their availability.
- *Signaling Route Management*: transmits information about routes availability (only for quasi-associated signaling mode).
- *Signaling Traffic Management*
  - Message Routing Control: includes the routing adjustment in order to warranting destination access or reestablishing normal routing.
  - Traffic Transfer Control.
  - Flow Control.

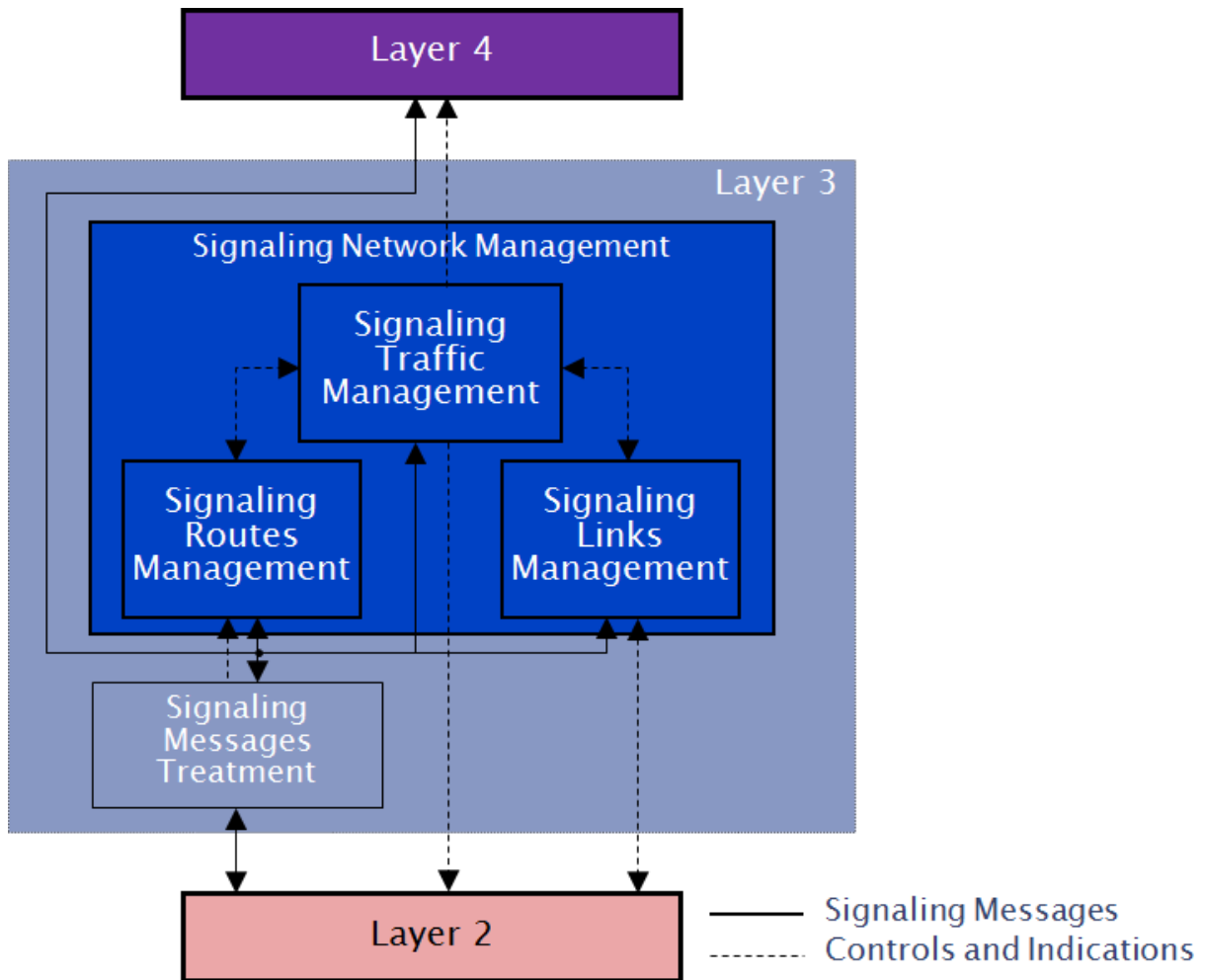


Figure A - 26. MTPL3 Signaling Network Management Functions.

Signaling Network Management (SNM) functions imply a SI value of «0». Then, the SIF contains, besides the routing label, the management information subfield. The latter is divided in one octet header and multiple octet indications, whose values are used for link/linkset, route/routeset and traffic management. Further description of these functions is beyond the scope of this work.

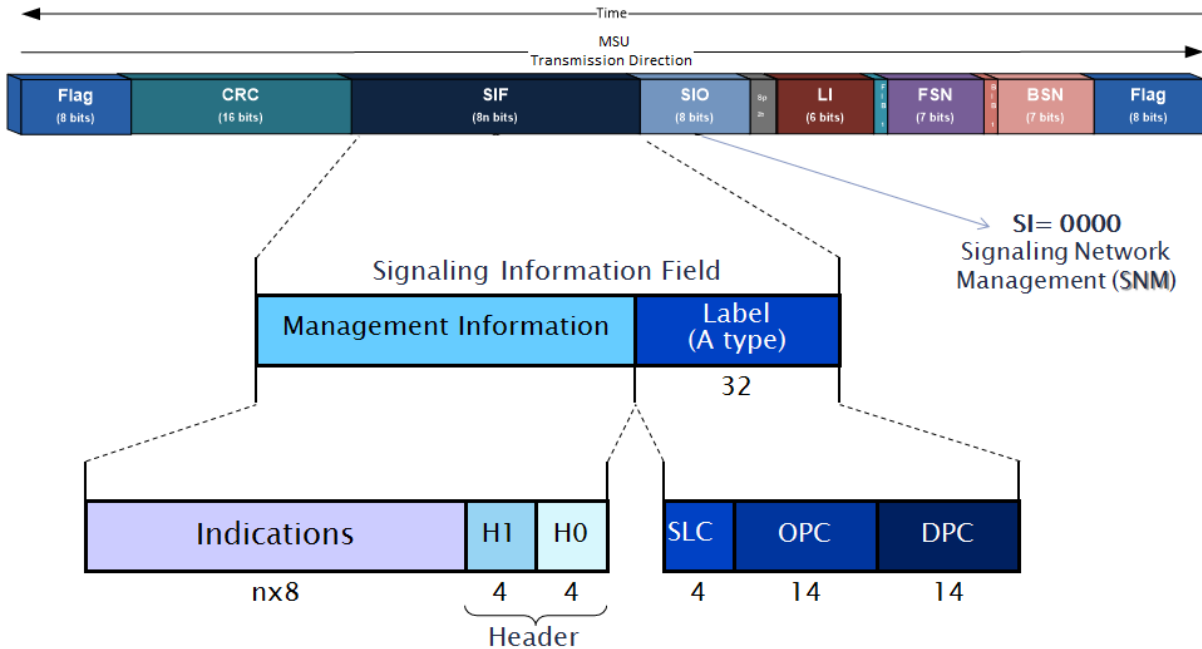


Figure A - 27. Signaling Network Management MSU Format.

#### A.3.1.4 Integrated Services for Digital Network User Part (ISUP)

ISDN (Integrated Services for Digital Network) constitutes a set of standards for the simultaneous digital transmission of voice, video, data and other network services over a Circuit-Switched Core Network (CS CN) within a PSTN (Public Switched Telephone Network), PLMN (Public Land Mobile Network) or within a PDN (Public Switched Data Network).

The ISDN integrates voice and data over the same transmission lines, adding services which were not available over the Plain Old Telephone System (POTS). Then, through a common access and network termination, an integrated access to

services and networks become available for home or corporate use through three type of channels:

- B (64 Kbps): voice and data.
- D (16/64 Kbps): signaling and low speed data.
- H (384/1.536/1.920 Kbps): video, high quality audio, high speed data, etc.

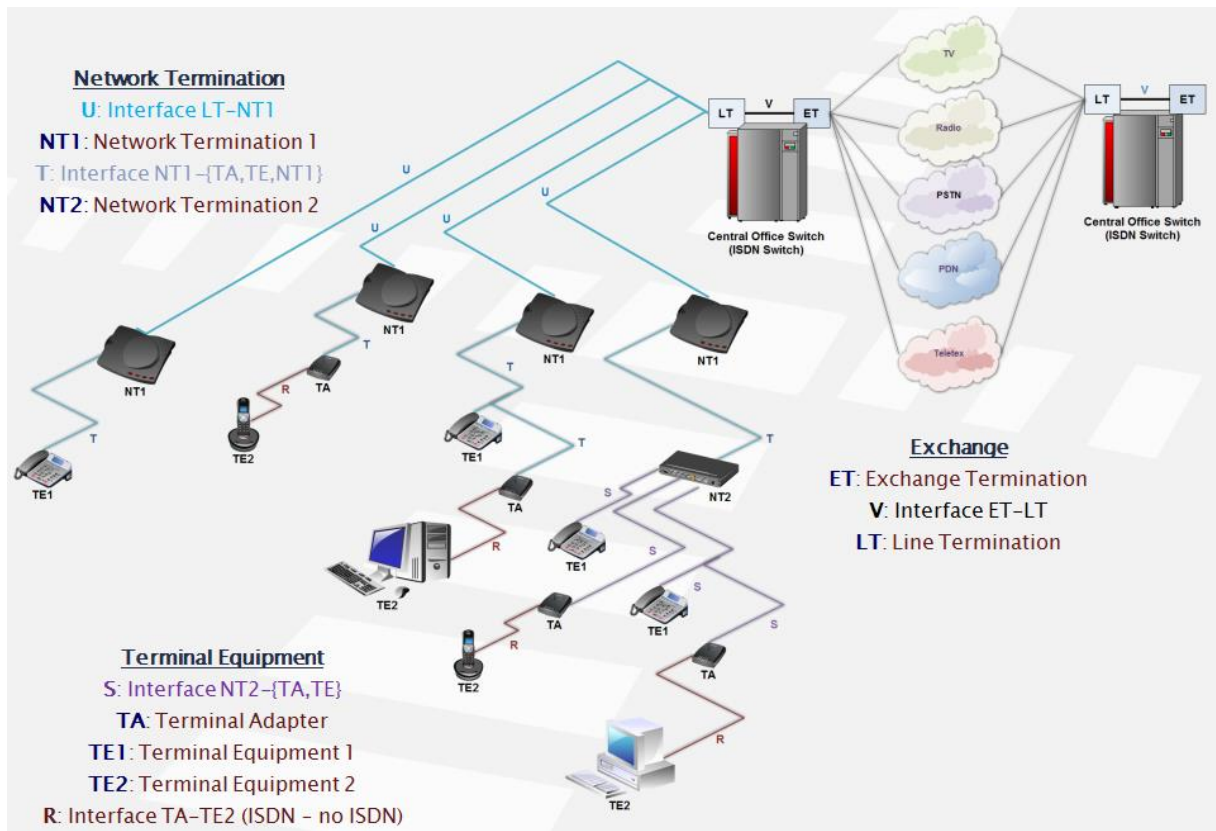


Figure A - 28. ISDN user-network access reference configuration.

Two types of Access are defined:

- BRI (Basic Rate Interface):
  - 2 B channels (64 Kbps) used for voice and data (maximum of 2 simultaneous conversations)
  - 1 D channel (16 Kbps) used for signaling and low speed data.
  - 144 Kbps Digital Subscriber Line (U interface).
  - SOHO (Small Office Home Office), maximum of 8 home terminals.
- PRI (Primary Rate Interface):
  - Digital Subscriber Line (U interface): 2048 Kbps (E1) or 1544 Kbps (T1)

- 30/23 64 Kbps B channels (Europe E1 / USA T1).
- 1 D 64 Kbps channels.

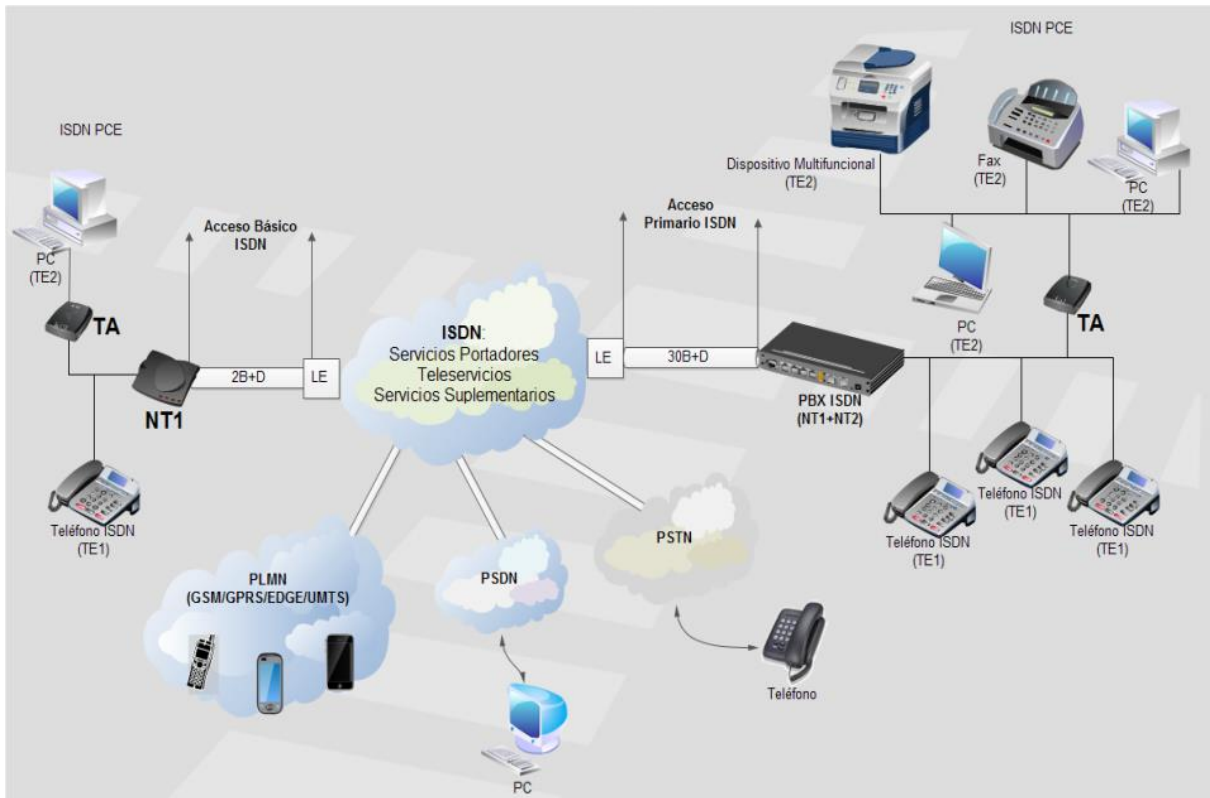


Figure A - 29. ISDN infrastructures/accesses.

ISDN can be divided in the following categories:

- Bearer Services: they only offer network capacity for data transfer.
  - 64 Kbps unrestricted (audio at 3.1 or 7 KHz, etc.).
- Teleservices: they use both network and terminals capacity.
  - Telephony;
  - Telefax;
  - Teletex;
  - Videotex, etc.

- Supplementary Services: they provide additional capabilities beyond basic services, namely:
  - CUG (Closed Users Group);
  - Call forwarding/Call transfer;
  - Do-Not-Disturb
  - Abbreviated dialling
  - Outgoing call barring (customer controlled)
  - Outgoing call barring (fixed)
  - Incoming call barring
  - Total call barring
  - Multiple subscriber numbering (MSN);
  - Three-way conference;
  - Billing information.

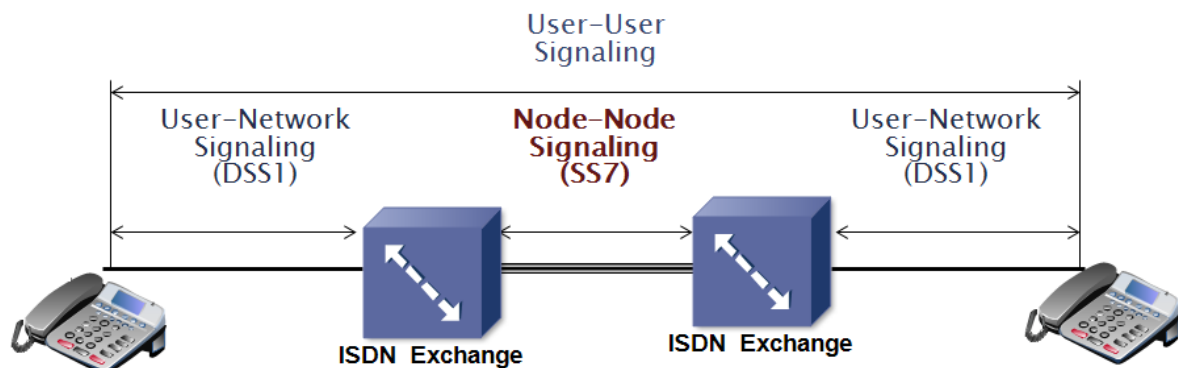


Figure A - 30. Signaling stages between ISDN users.

Node-Node signaling is supported by SS7 through the appropriate User Part for each Service. For Circuit-Switched telephony according to SS7 the available options are TUP (Telephone User Part) or ISUP (ISDN User Part). ISUP was adopted almost everywhere for telephony, mainly because of the following disadvantages against ISUP:

- TUP cannot transport information compatible with DSS1.
- User-User signaling is not specified in TUP
- Call suspension and resume is supported by ISUP but not in TUP.
- TUP does not support the amount of supplementary services offered by ISUP.

- Call on hold is not supported in TUP.
- Call release is not symmetric in TUP as it is in ISUP.

#### **A.3.1.4.1 ISUP Message Structure**

ISUP messages are carried on the signalling link by means of MSUs, where the Service Indicator is coded as 0101 (0x05).

The SIF of each MSU containing an ISUP message consists of an integral number of octets and encompasses the following parts:

- Routing label.
- Circuit Identification Code (CIC).
- Message type code.
- Mandatory fixed part.
- Mandatory variable part.
- Optional part, which may contain fixed length and variable length parameter fields.

Each ISUP message contains a mandatory part consisting of fixed length parameters, which could only comprise the type of message. The mandatory part might be continued by the mandatory variable part and/or an optional part.

The optional part includes parameters identified by a code followed by a one octet length indicator. This sequence of optional parameters might be repeated in an established order until the end of optional parameters indicator, consisting of one octet of value «0».

CIC identifies the voice/data channel which transport the call associated with the message. It allows associating the voice/data channel with the signaling channel.

For each individual circuit connection, the same routing label must be used for each message that is transmitted for that connection (SLS bits are set to the four least significant bits of the CIC).

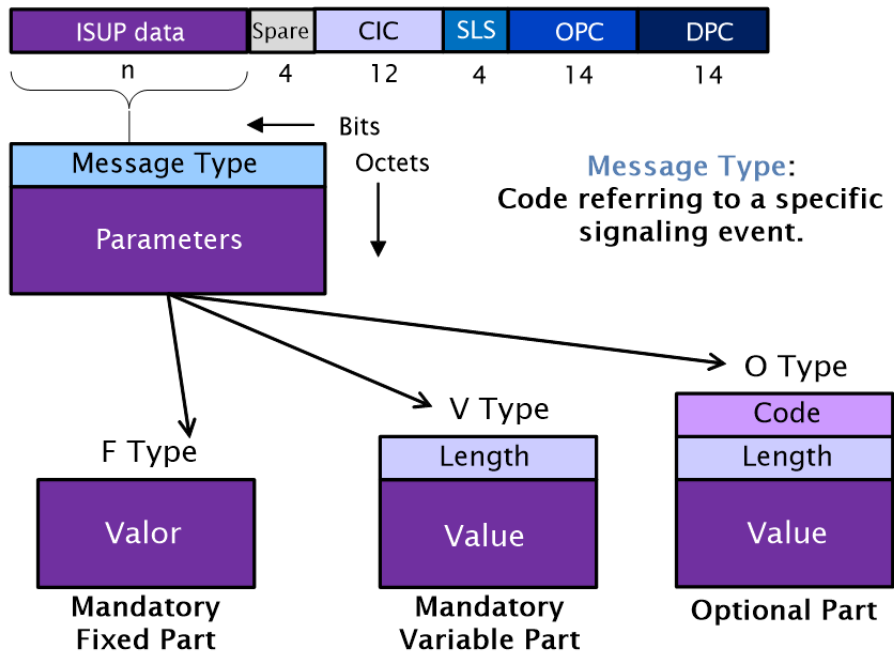
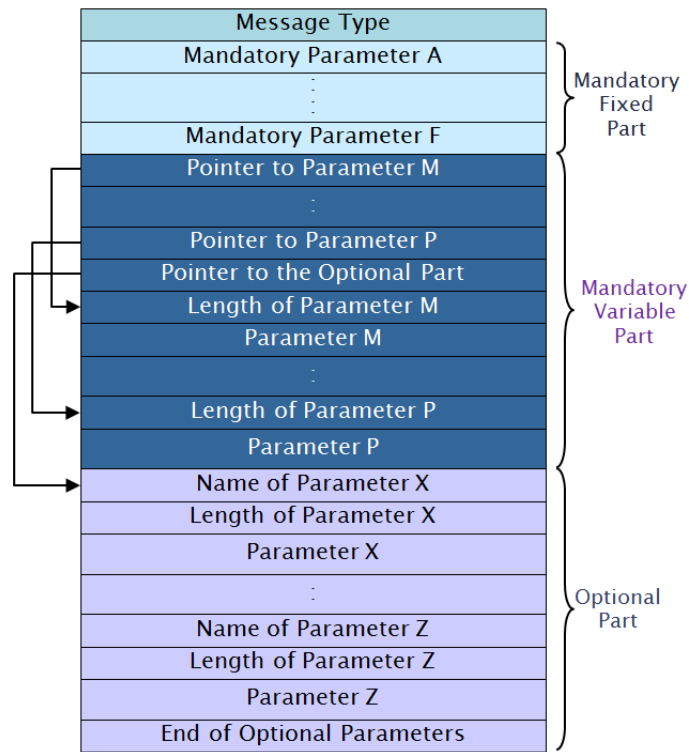


Figure A - 31. ISUP message structure embedded in MSU's SIF.

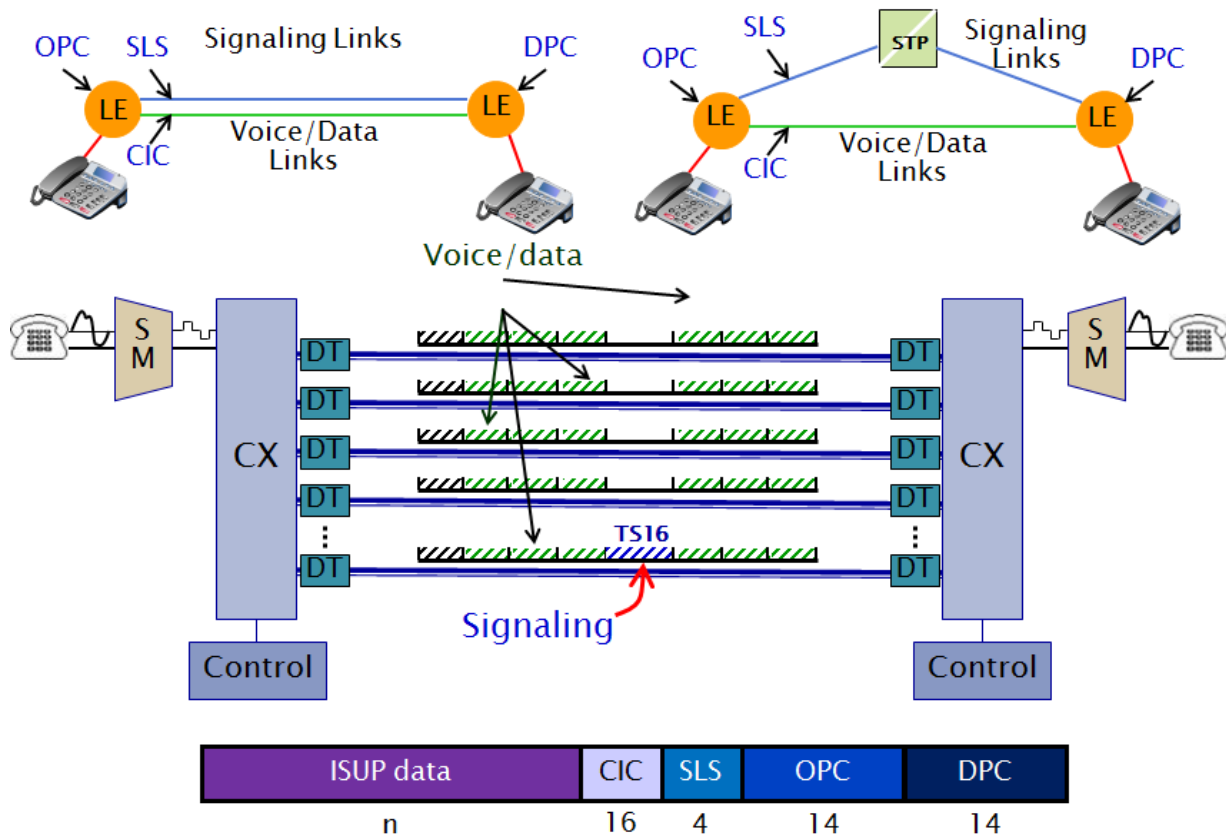


Figure A - 32. ISUP signaling transport via E1 between Local Exchanges (LE) subscribers, either for associated or quasi/non-associated signaling modes.

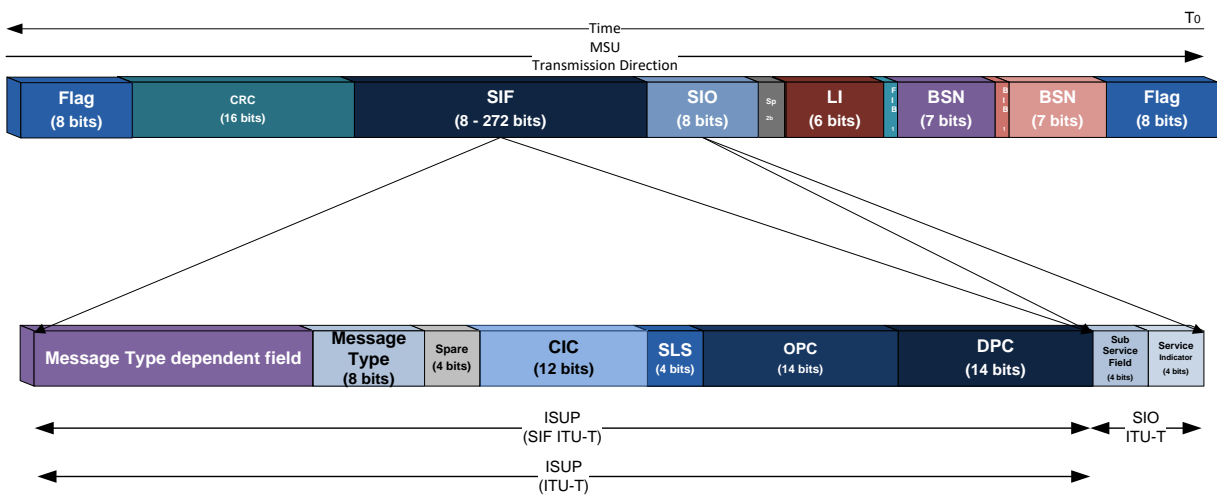


Figure A - 33. ISUP message encapsulation in SS7 MSU according to ITU-T.



**A.3.1.4.2 ISUP Call Signaling**

Message	Acronym	Description
Initial Address Message	IAM	Call establishment message
Subsequent Address Message	SAM	Call establishment message, remaining digits of the called party (B number) not fitting in IAM
Address Complete Message	ACM	Indicator of back tone reception by the called party (ringing)
Answer Message	ANM	Answered call message indicator
Release	REL	Released call message indicator
Release Complete	RLC	Call resources complete release indication
Call Progress	CPG	Call in progress message indication; might be used to indicate ringing or available online information
Connect	CON	Responded call message indication. CON might be used, for example, by an answering machine

Table A - 4. Basic call ISUP messages.

Table A-4 describes the set of ISUP messages used for basic ISDN call signaling.

Next call flow diagram of Figure A-34 exhibits an example of ISUP signaling between ISDN users during a call with unconditional forwarding. In this case, the called party included in the ISUP IAM message has already set to forward the call to another ISDN number (a mobile subscriber).

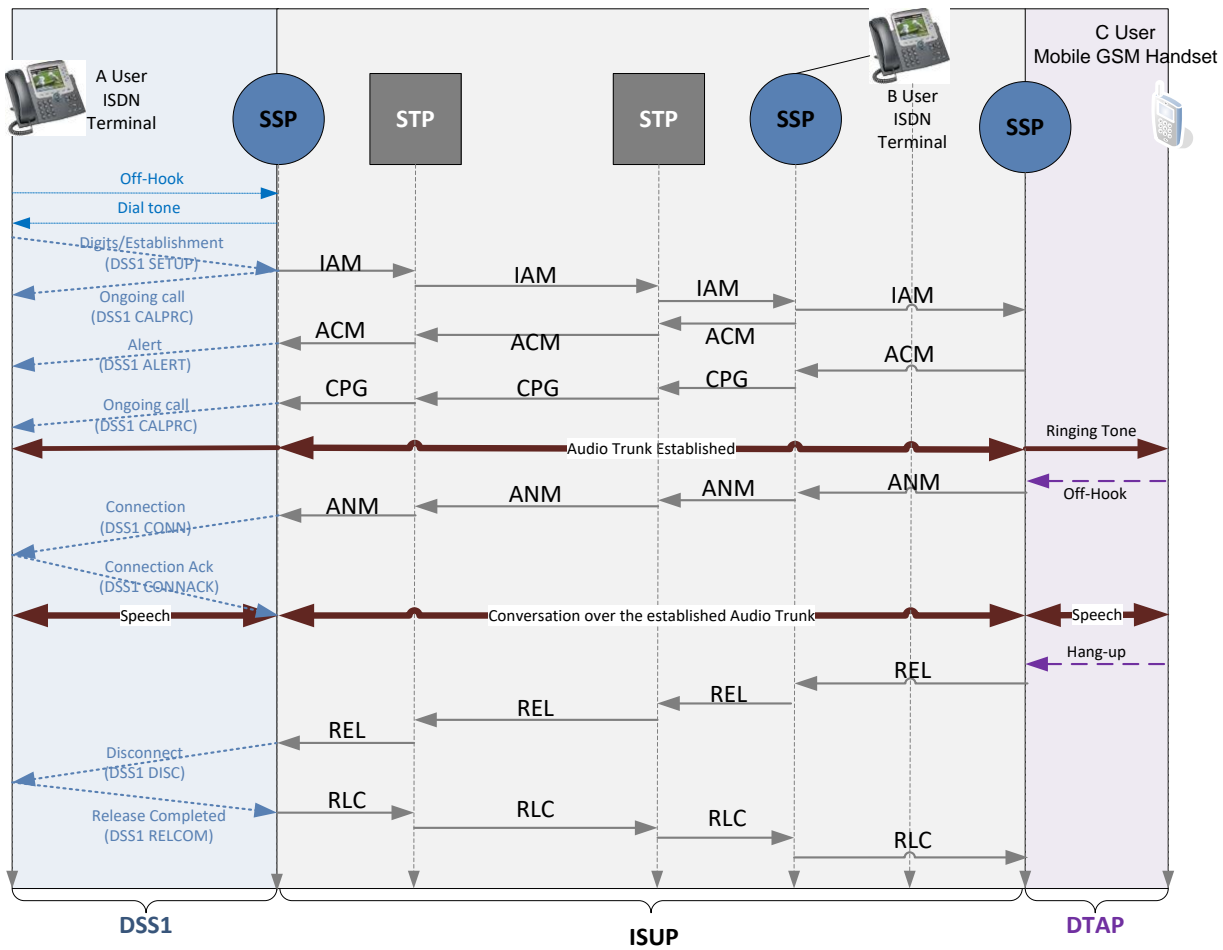


Figure A - 34. Unconditional Call Forwarding (UCF) signaling example.

#### A.3.1.4.2.1 Initial Address Message (IAM)

ISUP's IAM message, sent from the SSP attending the calling party, is used to complete the circuit between both parties of a call, origin and destination. The message contains the calling party number within the mandatory variable part, as well as it may contain the originating number (calling party) in the optional part.

Typically, it contains four F (fixed) type parameters (Nature of Connection indicators, Forward Call indicators, Calling Party (A) category, Transmission Medium requirement), one V (variable) type parameter (Called Party (B) number) and up to 56 O (optional) type parameters (Calling Party (A) number, Initial Called number,

etc.). Figure A-35 shows the ISUP IAM structure according to ITU-T. According to its position within an SS7 MSU, its structure has been enacted as the MSU's SIF components next to the SIO element (whose value is 5 for ISUP). These message is recognized by establishing the Message Type parameter vale as «1».

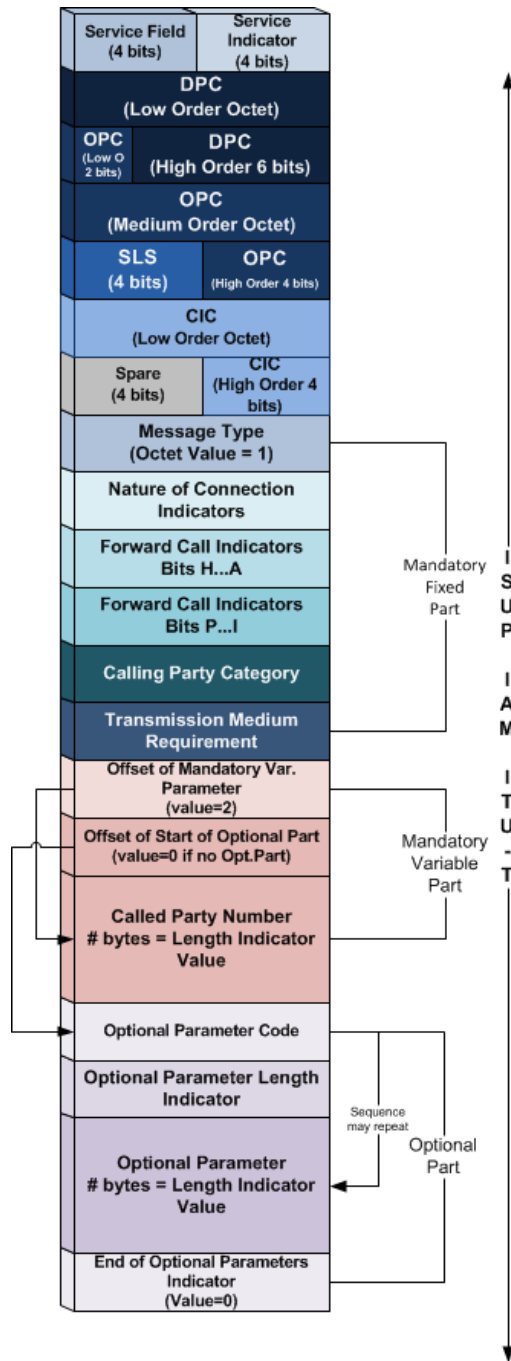


Figure A - 35. ISUP IAM message structure according to ITU-T.

### A.3.1.4.2.2 Address Complete Message (ACM)

ISUP's ACM message is sent in reverse direction from the SSP giving service to the call's destination part (Called Party), indicating a trunk circuit reservation at the destination remote end. The call's origin SSP answers to the ACM message connecting the trunk circuit of the calling party so as to completing the voice circuit, simultaneously sending a ringing tone to the destination subscriber line.

An ACM is typically composed of one F (fixed) parameter (Backward Call Indicators), no V (variable) parameters, and eventually O (optional) parameters. Figure A-36 shows ISUP ACM structure according to ITU-T. Giving its position within an SS7 MSU, its structure has been enacted as the MSU's SIF components next to the SIO element (whose value is 5 for ISUP). These message is recognized by establishing the Message Type parameter vale as «6».

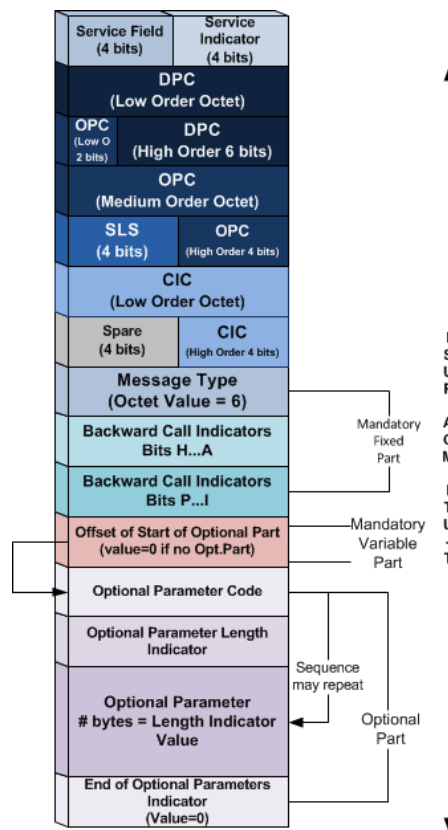


Figure A - 36. ISUP ACM message structure according to ITU-T.

### A.3.1.4.2.3 Answer Message (ANM)

When the called party answers, the destination SSP stops the ringing tone and sends back an ISUP ANM message to the origin SSP. After confirming both parties' connection to the reserved voice circuit, the charging process begins (something that could be done through a CDR -Call Detail Record- of computation data addition processed by a Billing center, controlled by an SCP, etc.).

An ANM is typically composed of no F (fixed) or V (variable) type parameters, and eventually O (optional) type parameters. Figure A-37 shows ISUP ANM structure according to ITU-T. According to its position within an SS7 MSU, its structure has been enacted as the MSU's SIF components next to the SIO element (whose value is 5 for ISUP). These message is recognized by establishing the Message Type parameter value as «9».

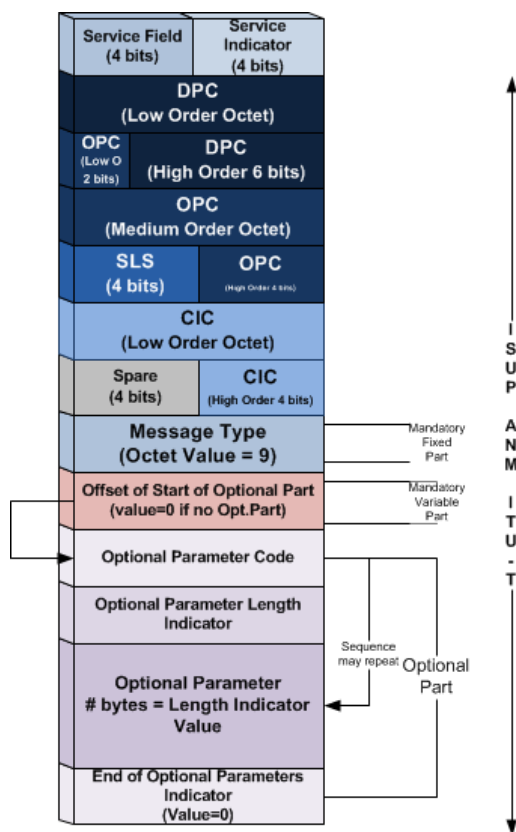


Figure A - 37. ISUP ANM message structure according to ITU-T.

### A.3.1.4.2.4 Release Message (REL)

ISUP's REL message is sent from the part which is releasing the call so as to indicate the established trunking circuit release. The Release Cause is included in the mandatory fixed part of the message within the Release Cause Indicator Parameter.

An ISUP REL is typically composed of no F (fixed) type parameters, one V (variable) type parameter (Release Cause Indicator), and eventually O (optional) type parameters. Figure A-38 shows the ISUP ANM structure according to ITU-T. According to its position within an SS7 MSU, its structure has been enacted as the MSU's SIF components next to the SIO element (whose value is 5 for ISUP). These messages are recognized by establishing the Message Type parameter value as «12».

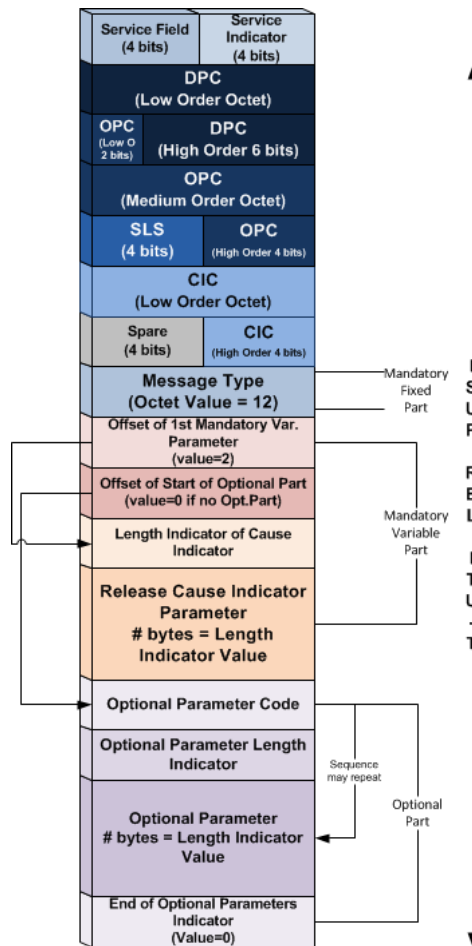


Figure A - 38. ISUP REL message structure according to ITU-T.

**A.3.1.4.2.5 Release Complete Message (RLC)**

ISUP RLC message is sent in the reverse direction of the REL message, as a voice trunk circuit release acknowledgement, and at the same time, appropriate billing process termination.

An RLC contains neither F (fixed), nor V (variable) nor O (optional) type parameters. Figure A-39 shows ISUP RLC structure according to ITU-T. According to its position within an SS7 MSU, its structure has been enacted as the MSU's SIF components next to the SIO element (whose value is 5 for ISUP). These message is recognized by establishing the Message Type parameter vale as «16».

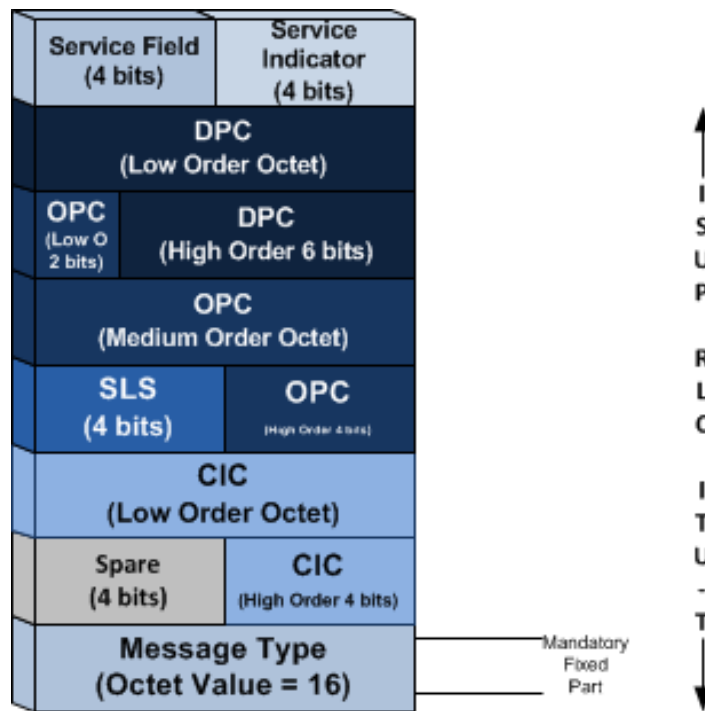


Figure A - 39. ISUP RLC message structure according to ITU-T.

### A.3.2 Signaling Connection Control Part (SCCP)

SCCP Layer (Signaling Connection Control Part), most of all performs routing functions additional to MTPL3. It is specified by the following:

- ITU-T Q.711 to Q.716
- ETSI EN 300 009-1
- ANSI T1.112

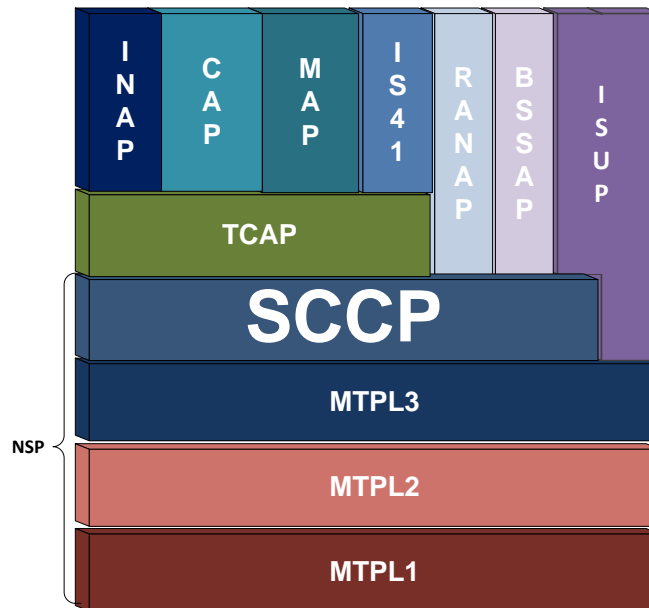


Figure A - 40. SCCP placement in SS7 protocol stack.

SCCP and MTPL3 combination is named as NSP (Network Service Part) in SS7. SCCP supplements MTP by providing both connectionless and connection-oriented network services for circuit-related and non-circuit-related information transfer.

SCCP can control logical signaling connections. It can also transfer signaling data across the network, with or without use of logical connections, becoming the transport layer of its immediate superior SS7 stack layer, i.e. TCAP.



**A.3.2.1.1 Routing based on SSN/DPC**

MTP layer only uses the destination SPC (DPC) for identifying the destination entity of SS7 messages, meanwhile SCCP uses further discriminative routing methodologies, allowing access to distinct applications or databases residing within signaling entities with the same SPC.

SCCP uses identifiers known as Sub System Number (SSN). An SSN allows then routing messages to different applications residing in an SS7 network entity addressed at MTPL3 by the same SPC. Each application or database has its unique assigned SSN within the signaling entity. SCCP addresses the message target application or database by the combination of the DPC (found in the Routing Label) and the SSN (found in the Called Party Address).

Given the fact that the SSN is represented by an only octet within the MSU structure, a maximum of 256 subsystems may be assigned to a particular SPC.

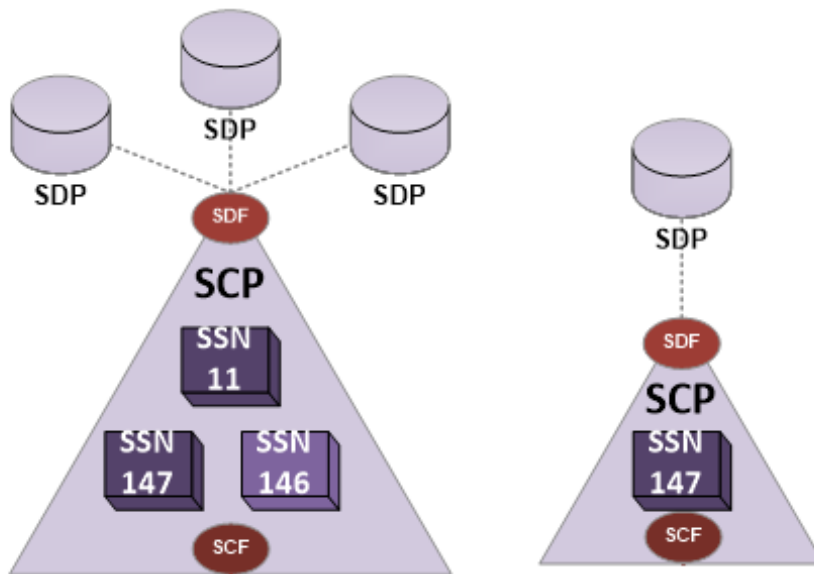


Figure A - 41. Service Control Points with one or several SSN.

### A.3.2.1.2 Routing based on Global Title Translation

Apart for routing based on SSN/DPC, the other SCCP routing procedure is the one known as Global Title Translation (GTT). A Global Title (GT) comprises a group of digits used by SCCP when routing based only on SSN/DPC becomes unfeasible. It constitutes the joint of a telephone directory number plus interpretation information of itself. It might be said it is the address used when the entity requiring information is not aware of the destination address. Hence, a Global Title implies the need for translation.

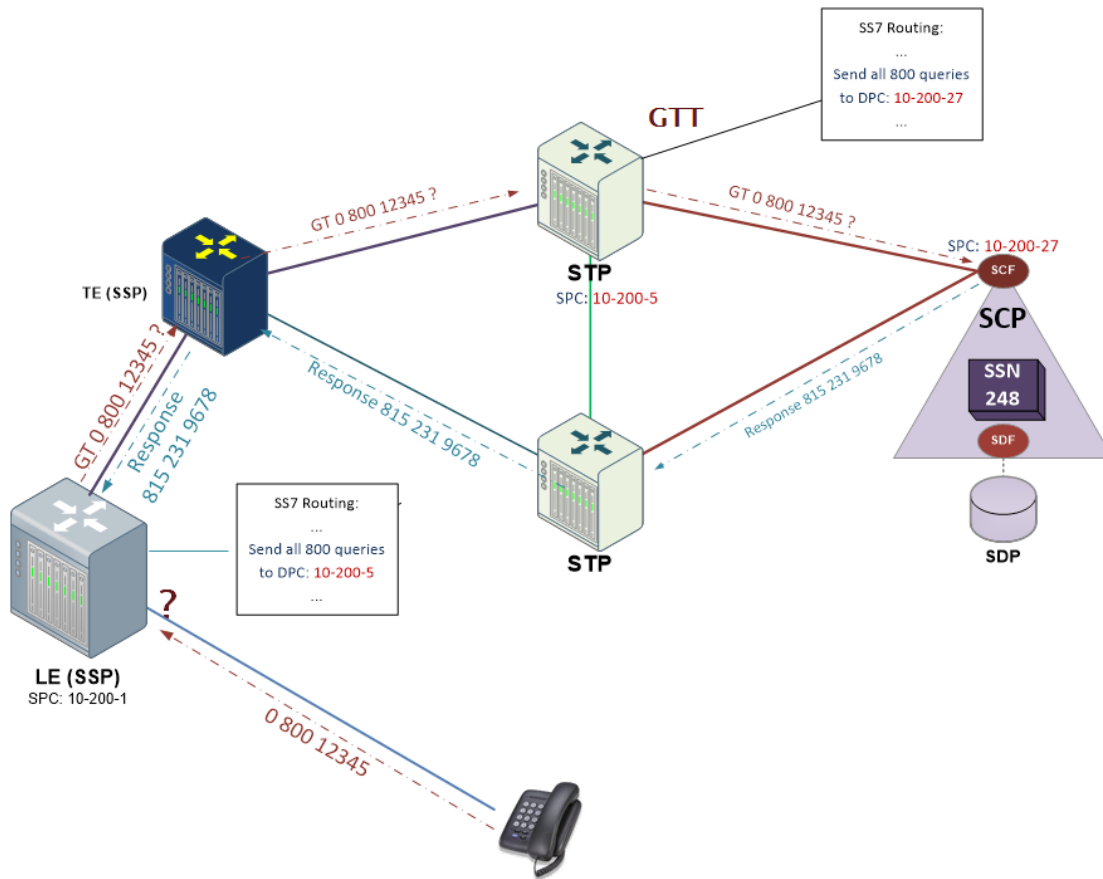


Figure A - 42. Global Title Translation example for 0800 dialing.

Service switching points or SCCP nodes, usually do not possess an information source for routing purposes any different than the dialed telephone number, particularly for international interconnections. A message composed using a GT is then sent to an entity whose routing tables are pre-configured in order to

recognizing the provided destination with the needed functionality to send back the data requested from the originating node.

Within a specific network, a unique entity might lead with Global Titles. This entity will then act as a Gateway with other SCCP local or foreign network nodes, providing the useful ability of information retrieval by entities which are unaware of its location. This entity providing GTT functionality is always an STP node, which allows originating SPs being unaware of target nodes' SSN/DPC for the ongoing service. Besides, GTT represents a load alleviation concerning the information transport within the network and to reside at the SPs. Otherwise, given the continuous deployment of new services and network alterations, it would turn out to be unmanageable. Only the STPs need to keep a SPC/SSN database associated to specific services and possible recipient destinations.

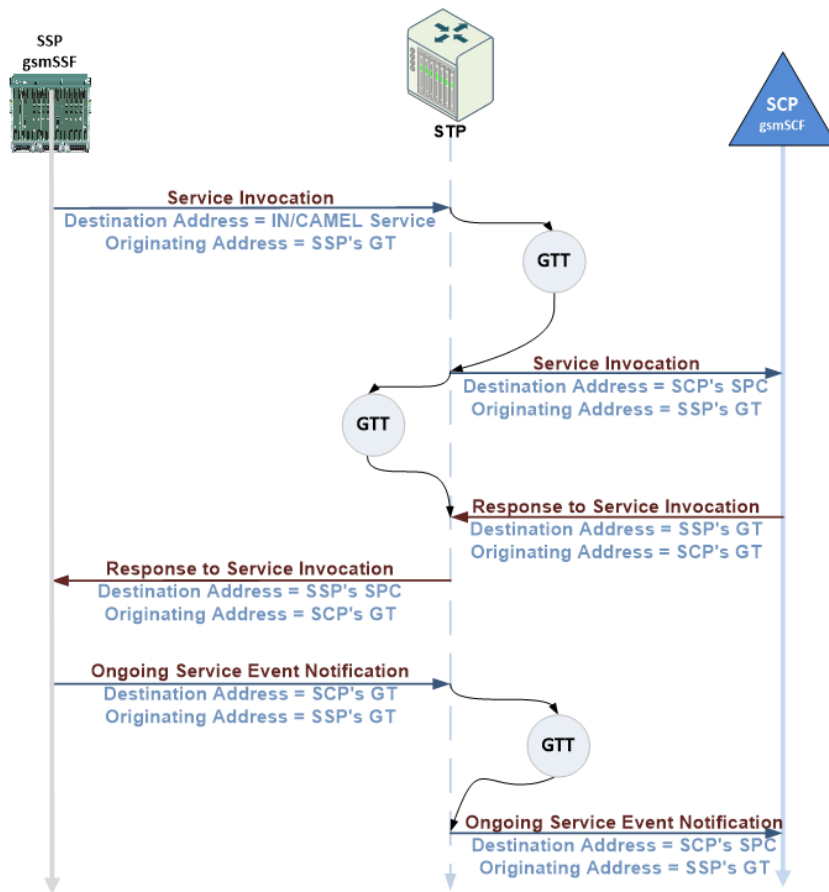


Figure A - 43. IN/CAMEL service call flow between SSP and SCP with Global Title Translation at the STP.

### A.3.2.1.3 SCCP Management

SCCP provides functions for managing the status of SCCP subsystems. Most of SCCP data traffic consists in managing (monitoring/maintenance) the status of the registered network available subsystems. These functions are mainly used to inform other subsystems of the status of an SCCP subsystem and allowing a coordinated status modification of SCCP subsystems.

Acronym	Message Name	Code	Description
SSA	Subsystem Allowed	01	Sent to inform SCCP management at involved destinations that a formerly prohibited subsystem is now allowed.
SSP	Subsystem prohibited	02	Sent to inform SCCP management at involved destinations of a subsystem failure.
SST	Subsystem status test	03	Sent to verify the status of a subsystem that has been marked as prohibited.
SOR	Subsystem out-of-service request	04	Sent to permitting subsystems going out of service with no degradation of network performance.
SOG	Subsystem out-of-service grant	05	Sent in response to an SCCP management SOR message to report that the request has been accepted.

Table A - 5. SCCP Management messages.

### A.3.2.1.4 SCCP Message Structure

SIO's Service Indicator field is coded with decimal value 3 (binary 0011) to refer to SCCP. SCCP message body is contained within the SIF field of an MSU. The SIF field contains the routing label followed by the SCCP message body. An ANSI MSU would only differ by the SIF's Routing Label).

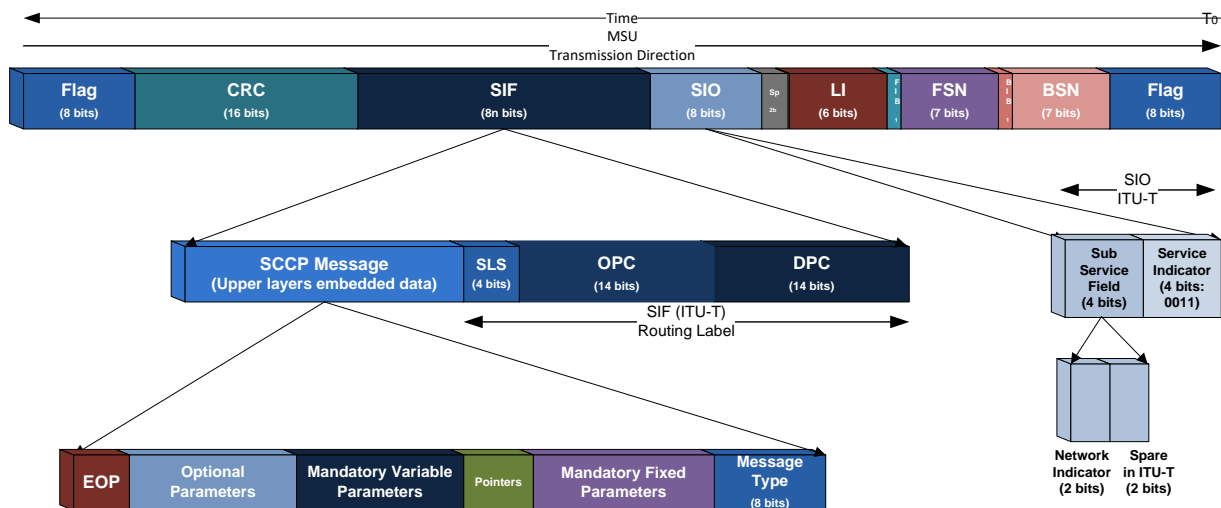


Figure A - 44. SCCP message structure and encapsulation in SS7 MSU (ITU-T).

SCCP message is composed of the following fields:

- **Message Type:** defines the message remaining content. It is one octet long and its possible values include:
  - 0x01=CR (Connection Request)
  - 0x02=CC (Connection Confirm)
  - 0x03=CREF (Connection Refused)
  - 0x04=RLSD (Released)
  - 0x05=RLC (Release Complete)
  - 0x06=DT 1 (Data Form 1)
  - 0x09=UDT (Unit Data). Connectionless-oriented messages used in GSM by MAP/TCAP for tasks transfer, as well as the radio interface, e.g: paging. Includes in its data structure:
    - 0x01=SSA (Subsystem Allowed)
    - 0x02=SSP (Subsystem Prohibited)
    - 0x03=SST (Subsystem Test)
    - 0x0A=UDTS (Unit Data Service)
    - 0x10=IT (Inactivity Test)
- **Mandatory Fixed Part.** The parameters of this part of the message are mandatory, of fixed length and keep a determined order. This permits the omission identifiers and length indicators. It includes:

- Protocol Class (1 octet):
  - Class (bits 0-3): indicates if connection-oriented (values 2,3) or connectionless-oriented (values 0,1). GSM MAP only uses values 0 or 1.
  - Message Handling (bits 4-7): indicates if a UDT type message should be answered in case of errors, used only for Class = 0 or 1.
- **Pointers:** Every pointer is one octet long and indicates the distance to the parameter at which it points to. Needed for every mandatory variable parameter, meanwhile only one pointer is needed for pointing the beginning of the optional parameters part.
- **Mandatory Variable Parameters:** The parameters of this part of the message are mandatory and in a fixed order, although its length is variable. Identifiers are not needed, but length indicators do for positioning of the parameters within the message. The length indicator uses an additional octet for each parameter.
- **Optional Parameters:** All parameters of this section are optional, depending on the submission circumstance. So as to enable optional parameters identification by the receptor of the message, an identifier and a length indicator of each optional parameter present in the message are needed.
- **EOP (End of Optional Parameters):** Every SCCP message with optional parameters must have this indicator so as to determine the end of them within the message structure. It is coded as "00", which obliges excluding it as a valid identifier.

#### A.3.2.1.4.1 SCCP Calling/Called Party Address

Either the Calling Party Address (CaPA) or the Called Party Address (CdPA), take part of the mandatory variable parameters of an SCCP message and have an identical structure, identifying the address type as well as the address itself, consisting of a series of elements as depicted in the Figure A-45 (ITU-T) and Figure A-46 (ANSI).

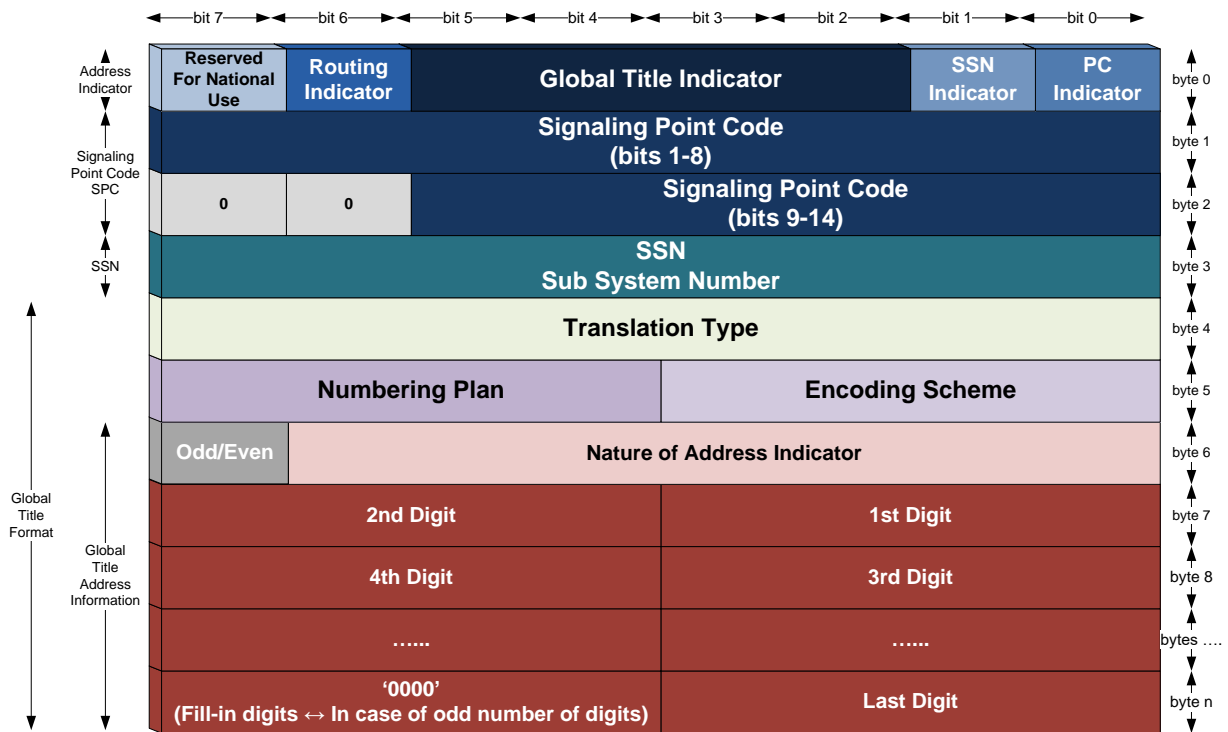


Figure A - 45. SCCP Calling/Called Party address structure (ITU-T).

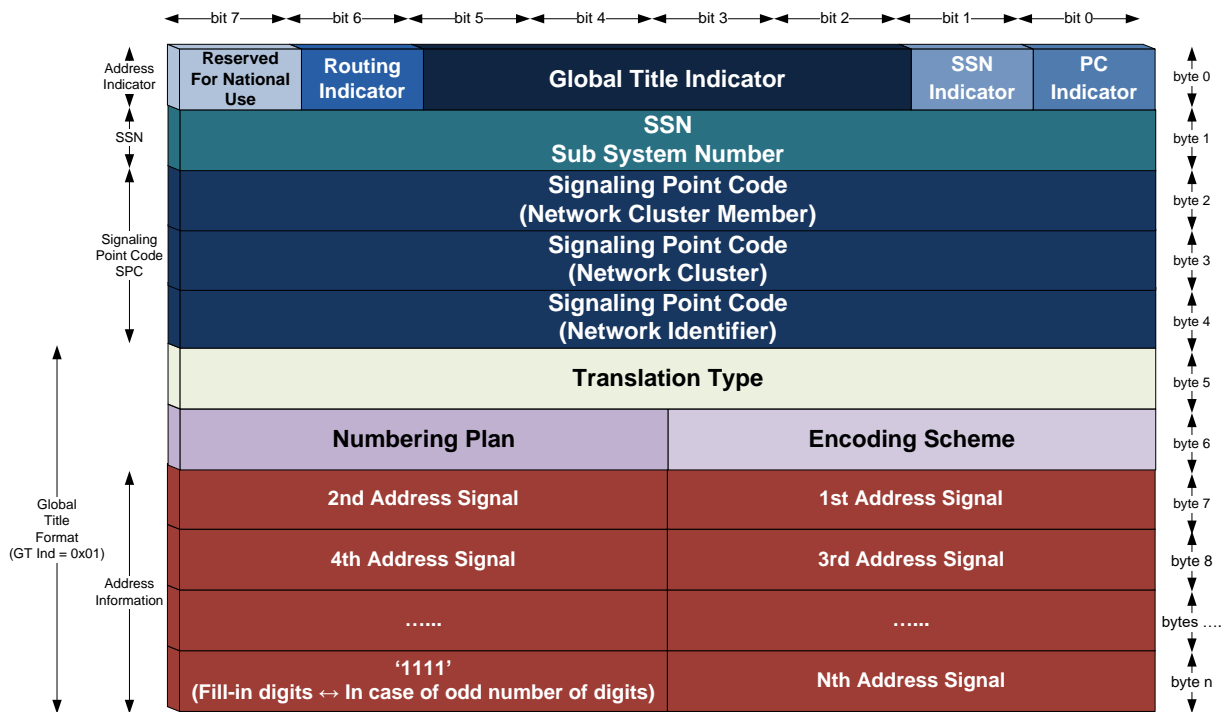


Figure A - 46. SCCP Calling/Called Party address structure (ANSI).

### A.3.2.1.4.1.1 Address Indicator (AI)

The first octet of either CaPA or CdPA constitutes a field known as Address Indicator. It forecasts the type of address information to be found in the address field. This address information can be a single type of address or any combination of SPC, GT and SSN. It tells the receiving entity which kind of address information to look for.



Figure A - 47 SCCP Address Indicator.

Each field of the Address Indicator and its significance are explained next:

- **PC Indicator:** specifies if the address includes or not a Signaling Point Code (SPC), according to the following values:
  - 0: the address does not include an SPC.
  - 1: the address includes an SPC.
- **SSN Indicator:** specifies if the address includes or not a un Sub System Number (SSN), according to the following values:
  - 0: the address does not include an SSN.
  - 1: the address includes an SSN.
- **Global Title Indicator:** specifies the Global Title (GT) composition according to the next table coding.

<b>Global Title Indicator</b>		
<b>Binary Value</b>	<b>ITU-T Meaning</b>	<b>ANSI Meaning</b>
0000 (0)	<i>Global Title is not included in the address</i>	<i>Global Title is not included in the address</i>
0001 (1)	<i>The Global Title only includes Nature of Address</i>	<i>Global Title includes Translation Type, Numbering Plan and Encoding Scheme.</i>



0010 (2)	<i>Global Title only includes Translation Type</i>	<i>Global Title only includes Translation Type</i>
0011 (3)	<i>Global Title includes Translation Type, Numbering Plan and Encoding Scheme</i>	<i>Not assigned</i>
0100 (4)	<i>Global Title includes Translation Type, Numbering Plan, Encoding Scheme and Nature of Address</i>	<i>Not assigned</i>
0101 (5) – 0111 (7)	<i>Spare International</i>	<i>Spare International</i>
1000 (8) – 1110 (14/E)	<i>Spare National</i>	<i>Spare National</i>
1111 (15/F)	<i>Reserved for extension</i>	<i>Reserved for extension</i>

Table A - 6. SCCP Global Title Indicator field values meaning.

- **Routing Indicator:** specifies the routing type used, according to the following values:
  - **0:** Route on Global Title, therefore, GTT is required. Routing is based on the Global Title found in the SCCP Called Party Address.
  - **1:** Route on SSN/DPC, therefore, a GTT is not required. Routing is based on the DPC (found in MTPL3 Routing Label at the SIF) and the SSN (found in the SCCP Called Party Address).
  
- **Reserved for National Use:** bit reserved for national or international use according to the following values:
  - **0:** International
  - **1:** National

Next table shows some Address Indicator example values and their meaning.

Address Indicator (ITU-T)			
Decimal	Hex	Binary	Meaning
16	10	00010000	Address does not include SPC Address does not include SSN GT includes Translation Type, Numbering Plan, Nature of Address and Encoding Scheme <b>Route on GT</b> International Network
17	11	00010001	Address includes SPC Address does not include SSN GT includes Translation Type, Numbering Plan, Nature of Address and Encoding Scheme <b>Route on GT</b> International Network
18	12	00010010	Address does not include SPC Address includes SSN GT includes Translation Type, Numbering Plan, Nature of Address and Encoding Scheme <b>Route on GT</b> International Network
19	13	00010011	Address includes SPC Address includes SSN GT includes Translation Type, Numbering Plan, Nature of Address and Encoding Scheme <b>Route on GT</b> International Network
67	43	01000011	Address includes SPC Address includes SSN Address does not include a GT <b>Route on SSN/DPC</b> International Network
82	52	01010010	Address does not include SPC Address includes SSN GT includes Translation Type, Numbering Plan, Nature of Address and Encoding Scheme <b>Route on SSN/DPC</b> International Network
83	53	01010011	Address includes SPC Address includes SSN GT includes Translation Type, Numbering Plan, Nature of Address and Encoding Scheme <b>Route on SSN/DPC</b> International Network

Table A - 7. SCCP Address Indicator value examples as for ITU-T.

**A.3.2.1.4.2 Signaling Point Code (SPC)**

The SPC correspondent to the Signaling Point Code of either a CaPA or a CdPA constitutes the SPC (OPC or DPC) embedded in the MTPL3 layer. This field comprises 3 bytes for ANSI and is located just after the SSN (bytes 2, 3, 4).



Figure A - 48. SCCP CaPA/CdPA Signaling Point Code field (ITU-T).

**A.3.2.1.4.3 Sub System Number (SSN)**

The SSN field of either a CaPA or CdPA comprises the subsystem number identifying an SCCP user function (for ANSI it's located just after the Address Indicator –byte 1-).

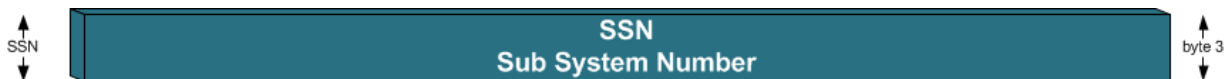


Figure A - 49. SCCP Calling/Called Party Address Sub System Number field (ITU-T).

SSN (Decimal Value / Network Entity)	
ITU-T Global Standard (GSM/UMTS Networks)	Network Entity
1	SCCP MG
6	HLR
7	VLR
8	MSC
9	EIR
10	AuC
ITU-T National Standard (GSM/UMTS Networks)	Network Entity
142	RANAP
143	RNSAP
145	GMLC (MAP)
146	gsmSCF (CAP)
147	gsmSCF (MAP) o IM-SSF (CAP)

148	SIWF (MAP)
149	SGSN (MAP)
150	GGSN (MAP)
249	PCAP
250	BSC (BSSAP-LE)
251	MSC (BSSAP-LE)
252	SMLC (BSSAP-LE)
253	BSS O&M (A interface)
254	(A interface)
ANSI (North America)	Network Entity
232	CNAM (Calling Name)
247	LNP
248	800 number translation (AIN0.1)
254	800 number translation (TCAP)

Table A - 8. Network entities SSN values.

#### A.3.2.1.4.4 Translation Type (TT)

The Translation Type parameter is used in a network to indicate the preferred method of GT analysis. Hence, it is used for routing the message to the appropriate Global Title Translation (GTT) function. Its value depends on the used higher layer protocol, embracing the meanings depicted in the following table.

<b>Translation Type</b>			
<i>Binary</i>	<i>Decimal</i>	<i>Hexadecimal</i>	<i>Meaning</i>
00000000	0	0	Unknown
00000001 - 00111111	1 - 63	1 – 3F	International Services
01000000 - 10000000	64 - 128	40 - 80	Spare
10000001 - 11111110	129 - 254	81 - FE	National Network Specific
11111111	255	FF	Reserved for expansion

Table A - 9. SCCP CaPA/CdPA Translation Type values meaning.

### A.3.2.1.4.5 Encoding Scheme (ES)

The Encoding Scheme field is used to indicate how the Global Title is coded, i.e. the number of digits the receiving node should recognize as part of the GT and how to translate these values from the binary code. This parameter value encompasses the meanings deployed in the following table.

<b>Encoding Scheme</b>				
Binary	Decimal	Hexa	ITU-T Meaning	ANSI Meaning
0000	0	0	<i>Unknown</i>	<i>Not used</i>
0001	1	1	<i>The address has an odd number of digits and should be converted to decimal values using Binary Coded Decimal (BCD) conversion</i>	<i>Binary Coded Decimal (BCD)</i>
0010	2	2	<i>The address has an even number of digits and should be converted to decimal values using Binary Coded Decimal (BCD) conversion</i>	<i>IA5</i>
0011	3	3	<i>National Specific</i>	<i>IP &amp; SS7 Addresses</i>
0100 - 1110	4 – 14	4 - E	<i>Spare</i>	<i>Reserved</i>
1111	15	F	<i>Reserved</i>	<i>Reserved</i>

Table A - 10. SCCP CaPA/CdPA Encoding Scheme values meaning.

### A.3.2.1.4.6 Numbering Plan

The Numbering Plan is used to indicate the type of numbering included in the address information. This parameter value encompasses the meanings deployed in the following table.

<b>Numbering Plan</b>				
Binary	Decimal	Hexa	ITU-T Meaning	ANSI Meaning
0000	0	0	Unknown	Unknown
0001	1	1	ISDN/telephony (Rec. ITU-T E.164)	

0010	2	2	Spare	Telephony Numbering Plan (C.163 & C.164)
0011	3	3	Data Numbering Plan (X.121)	Data Numbering Plan (X.121)
0100	4	4	Telex Numbering Plan (f.69)	Telex Numbering Plan (f.69)
0101	5	5	Maritime Mobile Numbering Plan (C.120 & C.211)	Maritime Mobile Numbering Plan (C.120 & C.211)
0110	6	6	Land Mobile Numbering Plan (C.212)	Land Mobile Numbering Plan (C.212)
0111	7	7	Mobile Numbering Plan (C.214)	Private Numbering Plan
1000 - 1100	8 – 12	8 – C	Spare	Reserved
1101	13	D	Reserved	Point Code & SSN
1110	14	E	Reserved	IP Routing
1111	15	F	Reserved	Reserved

Table A - 11. SCCP CaPA/CdPA Numbering Plan values meaning.

#### A.3.2.1.4.7 Nature of Address Indicator

The Nature of Address Indicator field is used by ITU-T to indicate the numbering nature included. This parameter value encompasses the meanings outlined in the following table.

<b>Nature of Address Indicator</b>			
Binary	Decimal	Hexadecimal	Meaning
0000000	0	0	Unknown
0000001	1	1	Subscriber Number
0000010	2	2	Reserved for National use
0000011	3	3	National Significant Number
0000100	4	4	International Number
0000101 - 1111111	5 - 127	5 – 7F	Spare

Table A - 12. SCCP CaPA/CdPA Nature of Address Indicator values meaning.

**A.3.2.1.4.8 Global Title Address Information (ITU-T)**

The Global Title Address Information (ITU-T) comprises the NAI field, the Odd/Even bit of the 6th byte of the CaPA/CdPA, plus the Digits of the Address Information field (whose format will depend on previously set TT, ES and NP fields values).

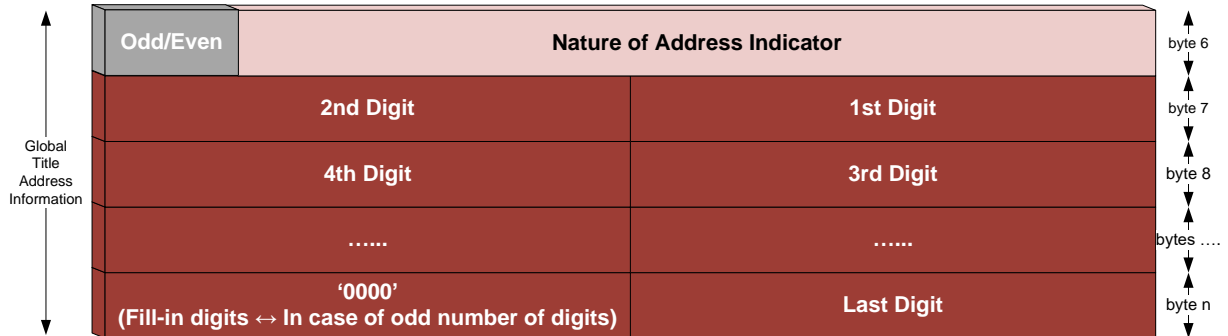


Figure A - 50. SCCP Global Title Address Information (ITU-T).

**A.3.2.1.4.9 Global Title Format and Address Information (ANSI)**

The Global Title Format (ANSI) approach is slightly different from ITU-T, comprising the Address Information field including the Address Signal digits preceded by potentially the TT, ES and NP fields according to the GTI (example below assumes GTI = 0001 = 1 = 0x01, thus GT includes TT, ES and NP).

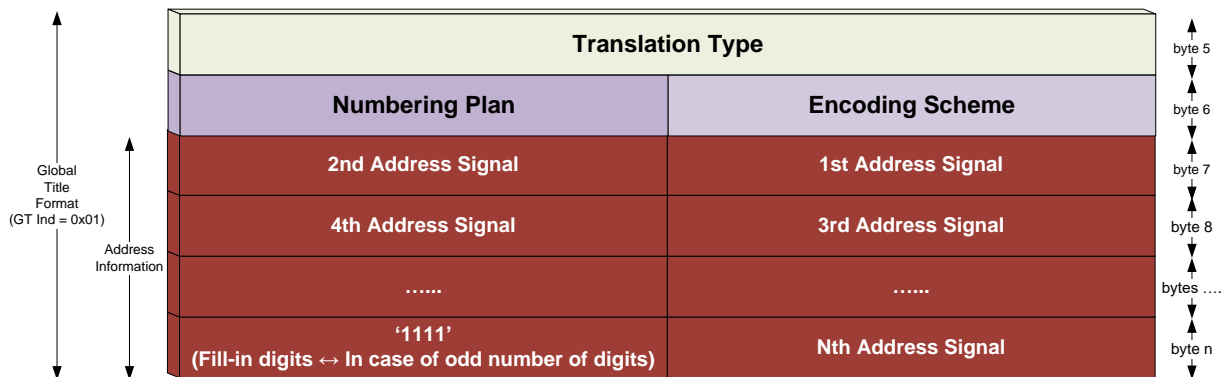


Figure A - 51. SCCP Global Title Format and Address Information (ANSI).

### A.3.3 Transaction Capabilities Application Part (TCAP)

TCAP layer offers a set of purely end-to-end communication proficiencies to its users, thus providing an interface between applications and a network layer service so as to accessing different service switching points and databases through SS7 on a global basis. Hence, it allows invoking advanced intelligent network services and modifying its parameters by supporting non-circuit related information exchange. TCAP is specified by the following:

- ITU-T Q.771 to Q.775
- ETSI EN 300 287
- ANSI T1.114

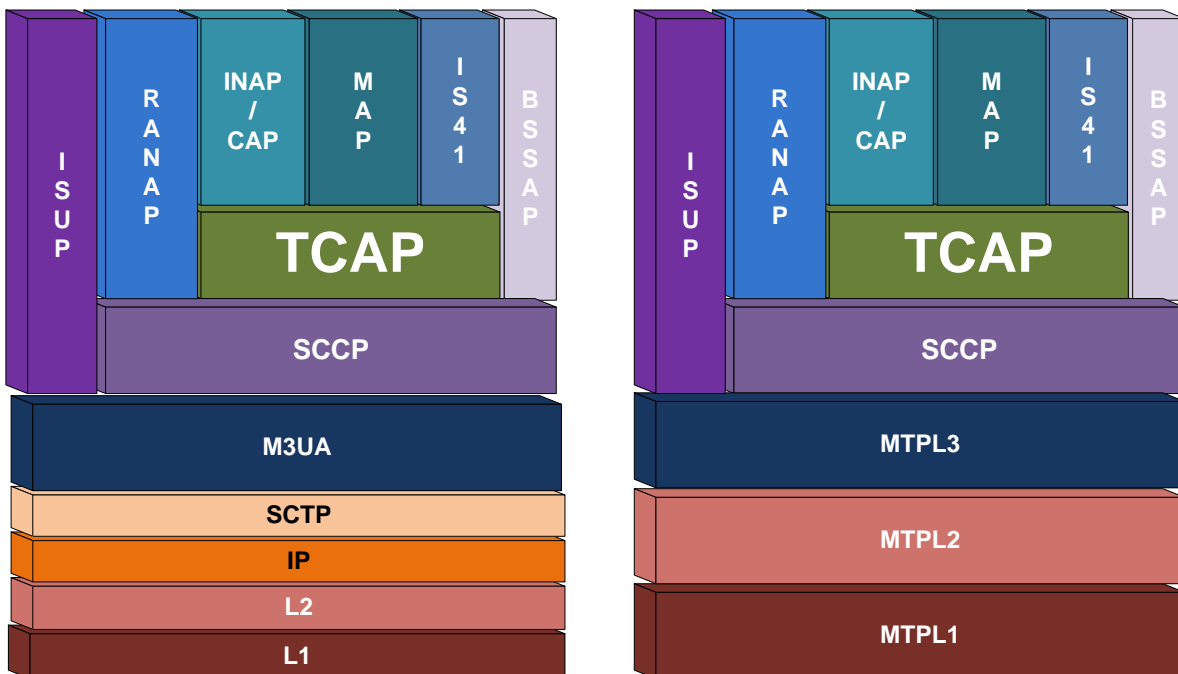


Figure A - 52. TCAP placement in SIGTRAN and pure SS7 protocol stack.

TCAP's primary purpose is facilitating multiple concurrent dialogs between the same Sub-Systems over the same machines, using Transaction IDs to differentiate these, similar to the way TCP ports facilitate multiplexing connections between the same IP addresses on the Internet.



TCAP uses SCCP as its transport layer under a specific structure of the data to be transferred. Likewise, it performs data flow control and presentation of results to SS7 upper layers.

TCAP scope should be considered for use between:

- Exchanges.
- An Exchange and a Network Service Centre (e.g. database, specialized facility unit, OA&M Centre).
- Network Service Centres.

TC-users (not exhaustive list):

- mobile service application (e.g. location of roamers);
- registration, activation and invocation of supplementary services involving specialized facility units (e.g. credit card service);
- non-circuit control-related exchange of signaling information (e.g. closed user group);
- operation and maintenance applications (e.g. query/response).

TCAP invokes queries (requests) and receives responses (indications). To ensure responses and queries correlation and correct order sorting, a numeric value (Invoke-Id) is inserted into each query invocation. The responding SP copies this number into its response so that query and response can be cross-referenced.

Each operation is identified by the Invoke-Id. Each indication is associated with the request based on the Invoke-id. The response can be a new operation request that is chained to the previous operation request using a link identifier.

Normally, all data parts and messages in TCAP are encoded according to the same scheme, with no distinction between mandatory and optional parameters.

TCAP supports four operation types:

- Class 1 - Both success and failure are reported.
- Class 2 - Only failures are reported.
- Class 3 - Only success is reported.
- Class 4 - Neither success, nor failure is reported.

Each operation is identified without ambiguity by the Invoke-Id. Each operation response (indication) is associated with the operation request by the Invoke-id, which is returned in a response to that operation invocation. If the response to an operation invocation is another operation invocation from the responding end, the original Invoke ID is returned as a Linked ID indicating that this responding operation invocation is "linked" to the original operation.

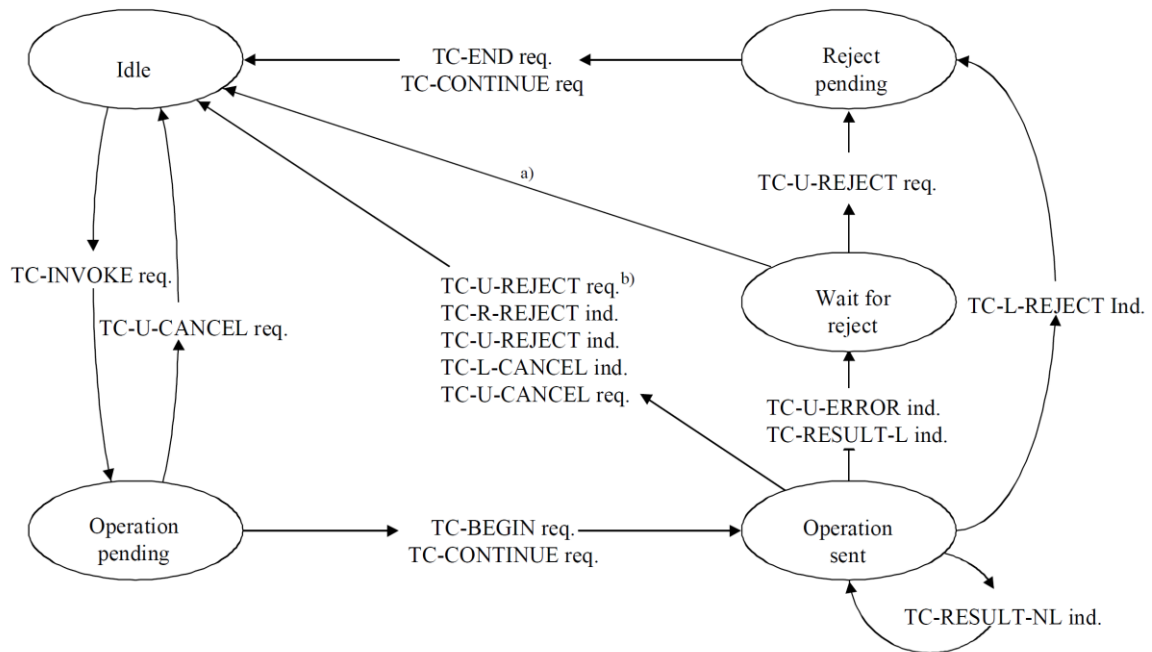
### A.3.3.1 TCAP Component States and State Transitions

For a given component ID, component correlation takes place only at the side which originates the operation; for this ID, component states and state transition diagrams are defined at this side only. The other side just reflects the value of the component ID in an Invoke or a Linked ID.

The following states are defined:

- **Idle:** No activity associated with the ID.
- **Operation Pending:** An operation has been passed to the Component sublayer, but no request for transmission has been issued.
- **Operation Sent:** An operation has been transmitted to the remote end, but no result has been received. The timer associated with the operation invocation (with the value of "Timeout") is started when the transition from "Idle" to "Operation Sent" occurs.
- **Wait for Reject:** The result has been received; TCAP is waiting for its possible rejection by the TC-user.
- **Reject pending:** Reject of the result has been requested by the TC-user, but no request for transmission has been issued.

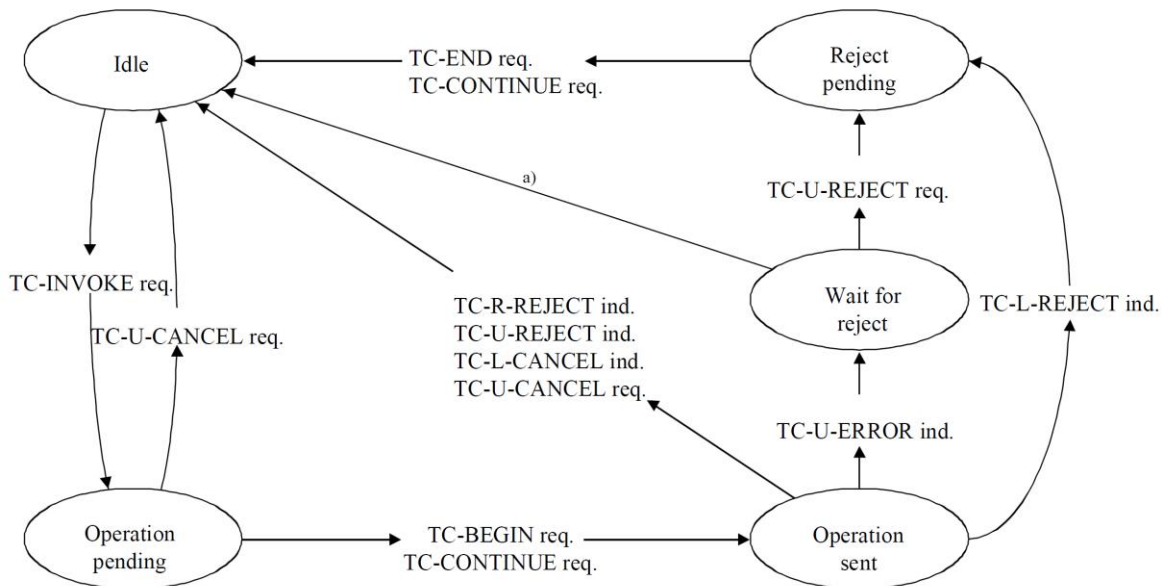
Class 1 operations (both success and failure reported)



- a) This transition is based on an implementation-dependent mechanism. The TC-user is not informed in this case.
- b) Provisionally accepted pending resolution of the issue that a TC-User can reject a segment of a result.

Figure A - 53 Class 1 Operations State Transition Diagram.

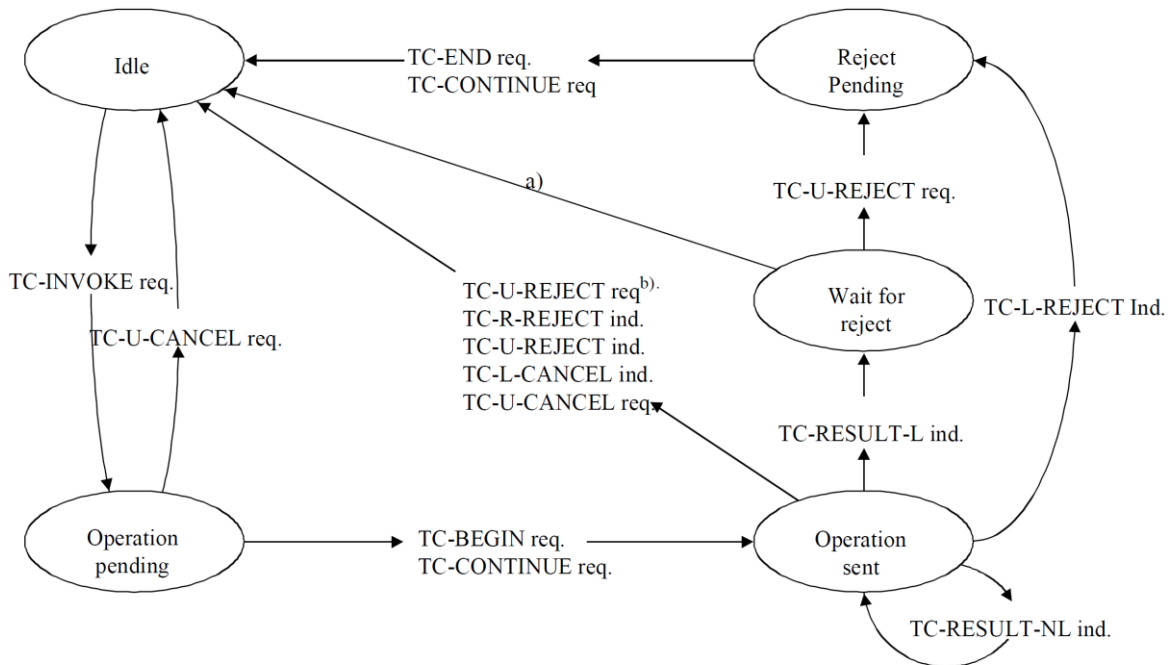
Class 2 operations (only failure reported)



- a) This transition is based on an implementation-dependent mechanism. The TC-user is not informed in this case.

Figure A - 54. Class 2 Operations State Transition Diagram.

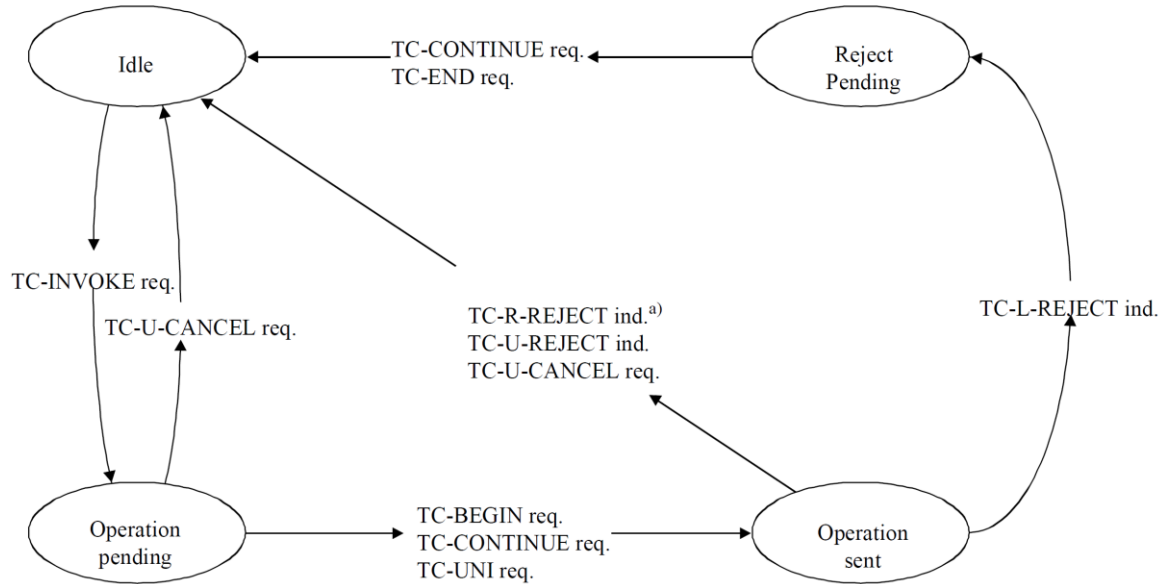
Class 3 operations (only success reported)



- a) This transition is based on an implementation-dependent mechanism. The TC-user is not informed in this case.
- b) Provisionally accepted pending resolution of the issue that a TC-User can reject a segment of a result.

Figure A - 55. Class 3 Operations State Transition Diagram.

Class 4 operations (neither success, nor failure reported)



- a) This transition can occur as a result of operation timeout expiry Notification to the TC-user is a local matter.

Figure A - 56. Class 4 Operations State Transition Diagram.

### A.3.3.2 TCAP Message Structure

All TCAP messages are embedded inside a fraction of a UDT SCCP message within an MSU. Hence, it uses connectionless-oriented SCCP services (ergo, SCCP fixed mandatory parameter «Protocol Class» equals 0 or 1).

A TCAP message is composed of the following functional sublayers known as portions, namely:

- **Transaction portion:** Responsible for operations and remote responses encapsulation. Components are Application Protocol Data Units (APDU) which carry the operations and responses and optionally, a dialog portion containing the application context or user information.
- **Component portion:** Allows components containing messages exchange between TC-users. A TC-user may send several components to the component sublayer before deciding sending all of them in a message alone. Thus, a TCAP message may carry several components.

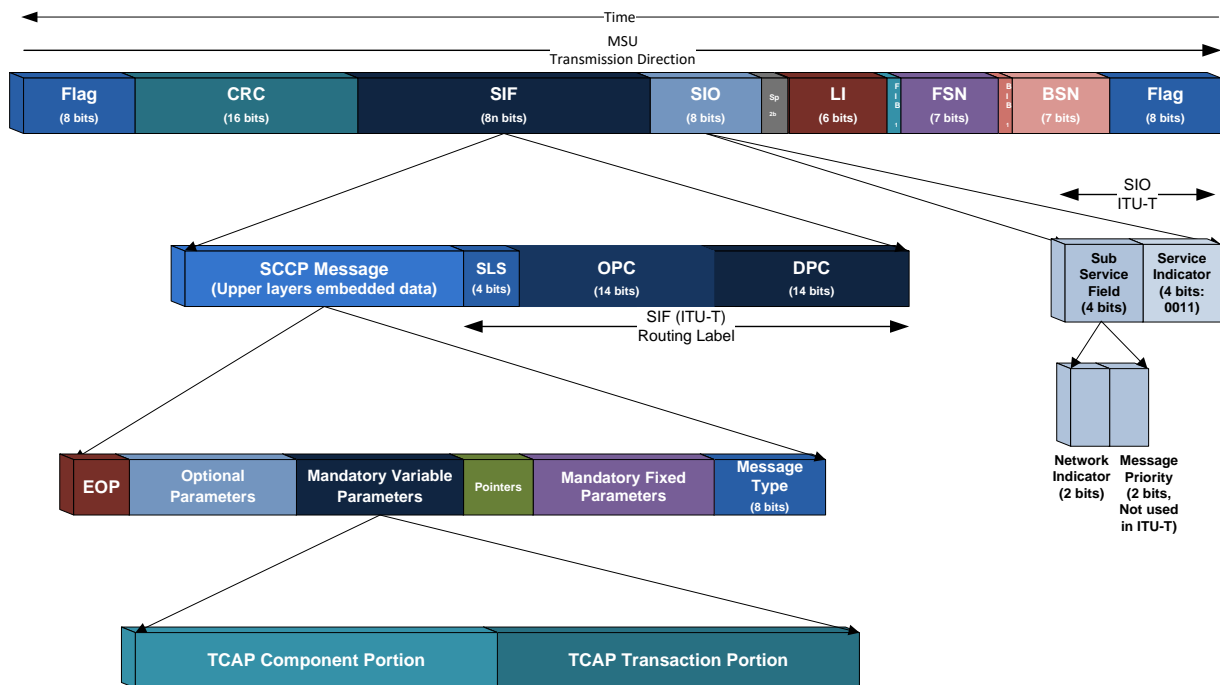


Figure A - 57. TCAP message structure and encapsulation in SS7 MSU (ITU-T).

A TCAP message is structured as a single constructor information element. It consists of a Transaction Portion which contains information elements used by the Transaction sublayer, and a Component Portion which contains information elements used by the Component sublayer related to components and, optionally, the Dialogue Portion which contains the Application Context and user information (which are not components).

One of the Transaction Portion elements is called the Component Portion, and it contains the Component sublayer information elements. Each Component is a constructor information element. The contents of each element are either one value (Primitive) or one or more information elements (Constructor).

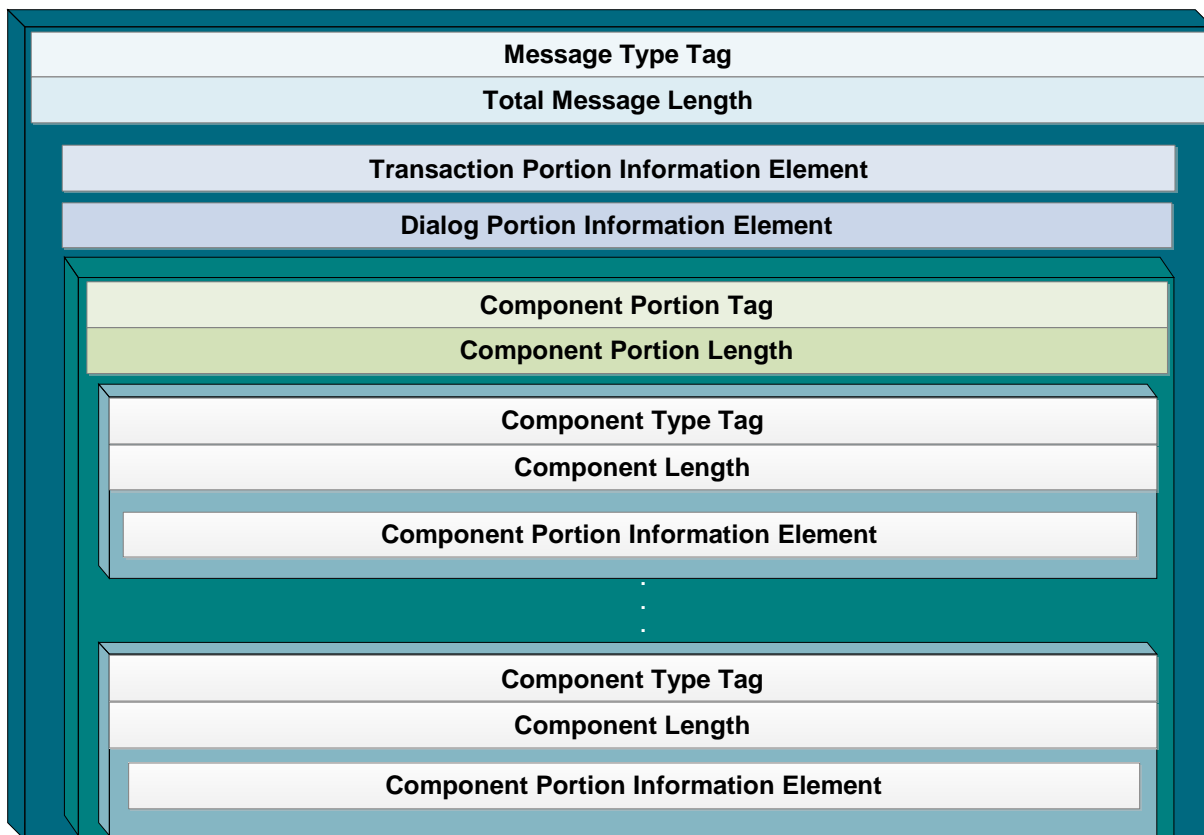


Figure A - 58. TCAP message general structure.

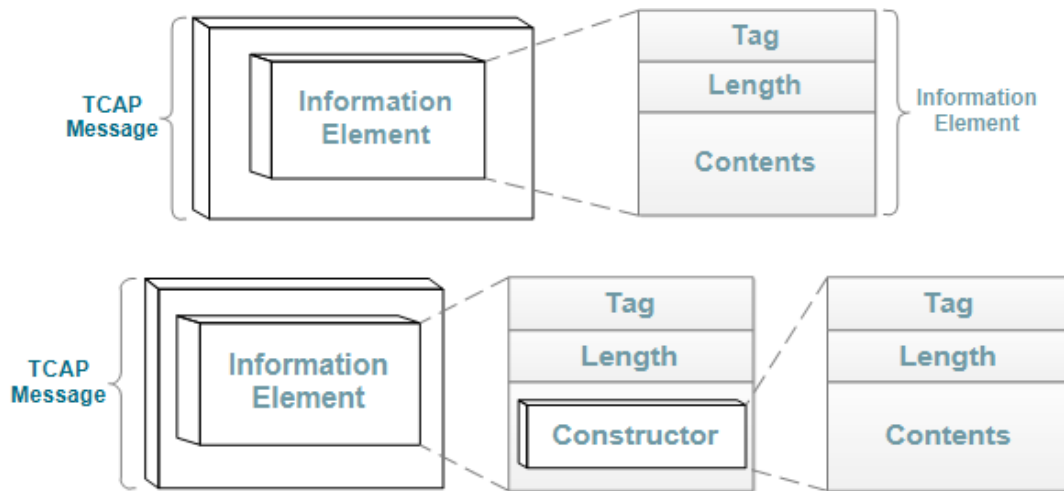


Figure A - 59. TCAP message information element structure.

### A.3.3.2.1.1 Transactional Sublayer (ITU-T)

ITU-T TCAP Transaction sublayer (TR) handles the interface to the network layer. There is a one-to-one relationship between dialogue handling primitives of the component sublayer and transaction handling primitives in the TR. The component handling primitives of the component sublayer have no counterpart in the TR.

ITU-T Q.771 – Primitives for the Transaction sublayer			
Name	Type	Parameters	
		Request	Indication
TR-UNI	Request Indication	Quality of Service (U) Destination Address (M) Originating Address (M) User Data (M)	Quality of Service (O) Destination Address (M) Originating Address (M =) User Data (M =)
TR-BEGIN	Request Indication	Quality of Service (U) Destination Address (M) Originating Address (M) Transaction ID (M) User Data (U)	Quality of Service (O) Destination Address (M) Originating Address (M =) Transaction ID (M) User Data (C =)
TR-CONTINUE	Request Indication	Quality of Service (U) Originating Address (O) Transaction ID (M) User Data (U)	Quality of Service (U) Transaction ID (M) User Data (C =)

TR-END	Request Indication	Quality of Service (U) Transaction ID (M) Termination (M) User Data (U)	Quality of Service (O) Transaction ID (M) User Data (C =)
TR-U-ABORT	Request Indication	Quality of Service (U) Transaction ID (M) User Data (U)	Quality of Service (O) Transaction ID (M) User Data (C =)
TR-P-ABORT	Request Indication		Quality of Service (O) Transaction ID (M) P-Abort (M)
TR-NOTICE	Request Indication	Quality of Service (U) Originating Address (O) Transaction ID (M) User Data (U)	Transaction ID (O) Originating Address (O) Destination Address (O) Report cause (M)

Table A - 13. Primitives for TCAP TR (ITU).

For previous table and hereinafter, the following convention applies when referring to type of primitive parameters:

- (M): mandatory parameter.
- (O): provider option.
- (C): conditional parameter (i.e. it will always be present in the indication type primitive if it was present in the corresponding request type primitive).
- (U): TC-user optional parameter.
- (=): the parameter must have the same value in the indication primitive as provided in the corresponding request primitive.
- A blank Indicates that the parameter is not applicable.

ITU-T TCAP TR definition of parameters follows:

- **Quality of Service:** The TR-user indicates the preferred Quality of Service. The "Quality of Service" parameters for the connectionless SCCP network service at present consist of the following:
  - *Return option:* specifies whether SCCP's "return message on error" is requested.



- *Sequence Control*: indicates that SCCP class 1 is requested and when used in a request primitive explicitly provides the information needed to deliver a series of messages in sequence.
- ***Destination Address***: Identifies the destination TR-user.
- ***Originating Address***: Identifies the originating TR-user.
- ***Transaction ID***: A transaction is identified by a separate transaction ID at each end.
- ***P-Abort***: cause of the abort of a transaction by Transaction sublayer.
- ***Termination***: Identifies the termination scenario chosen for the transaction (prearranged or basic).
- ***User Data***: Contains the information to be passed between TR-users.
- ***Report Cause***: Contains information indicating the reason for the exception report, that the message was returned by the SCCP with the reason as specified in Recommendation Q.711.

#### A.3.3.2.1.2 Transaction Portion (ANSI)

ANSI TCAP Transaction portion is composed as follows:

- ***Package Type Identifier***: Seven types of TCAP packages exist:
  - ***Unidirectional***: transfers components in only one direction, without expecting a response.
  - ***Query With Permission***: begins a TCAP transaction, which may be ended at the destination node.
  - ***Query Without Permission***: begins a TCAP transaction. The destination node is not obliged to respond it.
  - ***Response***: finalizes a TCAP transaction.
  - ***Conversation With Permission***: gives continuity to a TCAP transaction, which might be ended by the destination node.
  - ***Conversation Without Permission***: gives continuity to a TCAP transaction. The destination node is not obliged to respond or end it.
  - ***Abort***: finalizes a TCAP transaction due to an abnormal eventuality.
- ***Originating Transaction ID***: associates a TCAP transaction with a specific TCAP application at the originating SP.

- **Destination Transaction ID:** associates a TCAP transaction with a specific TCAP application at the destination SP.

#### A.3.3.2.1.3 Component Sublayer (ITU-T)

ITU-T TCAP Component sublayer is split into dialogue handling and component handling. Component handling primitives are defined as follows:

- **Invoke (TC\_INVOKE):** invokes an operation. The component may or not request a response.
- **Return Result Last (TC\_RESULT\_L):** returns the result of an operation. The component is the last information element of the result comprising the response of an Invoke.
- **Return Result Not Last (TC\_RESULT\_NL):** similar to «Return Result Last» with the difference that the response is followed by one or more further responses.
- **Return Error:** reports the unsatisfactory result of an operation invocation due to failure (TC\_U\_ERROR), local timeout (TC\_L\_CANCEL) or TC-user request (TC\_U\_CANCEL).
- **Reject:** indicates the reception of an incorrect component or package type. Component is rejected for some reason like duplicate invocation, unrecognized Linked Id, unrecognized operation or mistyped argument. Could be local reject (TC\_L\_REJECT), remote reject (TC\_R\_REJECT), user reject (TC\_U\_REJECT).
- **Reset (TC\_TIMER\_RESET):** Allows the local TC-user to refresh a timer of an operation invocation.

#### A.3.3.2.1.4 Component Portion (ANSI)

ANSI TCAP Component portion contains components, which include parameters containing specific information of no incumbency at the TCAP layer.

Six types of ANSI TCAP components exist, namely:

- **Invoke (Last)**: invokes an operation. The component is the last element of the query.
- **Invoke (Not Last)**: similar to «Invoke Last» with the difference that the component is followed by one or more components.
- **Return (Result Last)**: returns the result of an operation. The component is the last information element of the result.
- **Return (Result Not Last)**: similar to «Return Result Last» with the difference that the component is followed by one or more components.
- **Return Error**: reports the unsatisfactory result of an operation invocation.
- **Reject**: indicates the reception of an incorrect component or package type.

#### A.3.3.2.1.5 TCAP Message Types

TCAP message types involve the following:

- **BEGIN (BEG)**
  - Initiates/opens a TCAP dialog between TC-users (MAP, CAP, etc.).
  - BEG message contains the following mandatory fields:
    - Originating Transaction Identifier: identifies a dialog in TCAP's Transaction Portion assigned by the originating TC-user.
    - Invoke ID: can be used for dialog identification by the optional part at the TCAP Component Portion.
- **CONTINUE (CON)**
  - Used as transportation means between the beginning and ending of a data exchange process between TC-users (MAP, CAP, etc.). When a CON message is sent after a BEG message, it confirms protocol acceptance and requested application context.
  - CON message embraces the following mandatory fields:
    - Originating Transaction Identifier: identifies a dialog in TCAP's Transaction Portion assigned by the originating TC-user.

- Destination Transaction Identifier: identifies a dialog in TCAP's Transaction Portion assigned by the destination TC-user.
- **END**
  - TCAP END message is specifically sent when a process initiated by a BEG message needs to be terminated (occasionally, it may consist of a direct answer to the BEG message).
  - The END message, as optional part within the component portion could embrace additional application layer information (MAP, CAP, etc.)
  - END message embraces the following mandatory fields:
    - Destination Transaction Identifier: identifies a dialog in TCAP's Transaction Portion assigned by the destination TC-user.
- **ABORT (ABT)**
  - Either TCAP as its embedded application layer (MAP, CAP, etc.) may use the ABT message to spontaneously terminate a process given an error event or if an invocation could not be processed. The termination cause can be provided or not. Anyway, a source distinction is done for the termination.
  - When the TCAP service provider initiates a termination process P-ABORT is used. For this abort category, the ABT message provides a P-ABORT cause.
  - When the TC-user (MAP, CAP, etc.), initiates a termination, U-ABORT is used. For this abort category, a termination reason is sent within the Dialog Control field.
  - A frequent process termination resides in application layer (MAP, CAP, etc.) version incompatibilities (application context name) between dialog peers (one of them no longer supports it or is not yet compatible with the used version).
  - END message embraces the following mandatory fields:
    - Destination Transaction Identifier: identifies a dialog in TCAP's Transaction Portion assigned by the destination TC-user.

### **A.3.3.3 TCAP Dialog**

A TCAP dialog is established between itself and one of the upper layers usufructuary of its services. Within a specific dialog multiple active operations may reside. Each operation stores a result known as component, which can be stored by TCAP until discerning its discard post receiving a notification from a determined dialog handler indicator. Operations are identified and chained using the Invoke-Id.

When TCAP receives a message, it discriminates each component distinctly and individually sends them to the appropriate upper layer. As many simultaneous dialogs exist, each one is distinctly provided by an individual identity which is conserved by the components.

A TCAP transaction occurs when all the stored components related to a particular dialog are presented to the SCCP layer for transmission to the TCAP application particularly relevant for the occasion.

#### **A.3.3.3.1 TCAP Dialog types**

The term dialog portion has a different meaning from the mentioned TCAP dialog. A TCAP dialog refers to the complete information exchange process between TC-users.

It is important to discriminate structured from unstructured dialogs. GSM instance, only uses structured dialogs. The difference between both types of dialogs reside in the fact that unstructured constitute a unidirectional transmission of information, in which the originating entity does not expect an answer or any feedback. In contrast, a structured dialog consists of a beginning, an execution and a termination of the communication process among peers.

A TC-user opens a structured dialog when sending a BEG message. This message identifies a transaction (via the Originating Transaction Identifier). If the destination is enabled to accept the message, then it responds with a CON message, which contains identifiers for either message origin or destination

(Originating/Destination Transaction Identifier). Next, either parts may proceed to send additional messages. For ending a TCAP dialog, one of the ends sends an END message (SP 2 sends it in the underlying example, but it could obviously be sent in the inverse direction). Typically, a process results as short as the exchange of a BEG message followed by an END message.

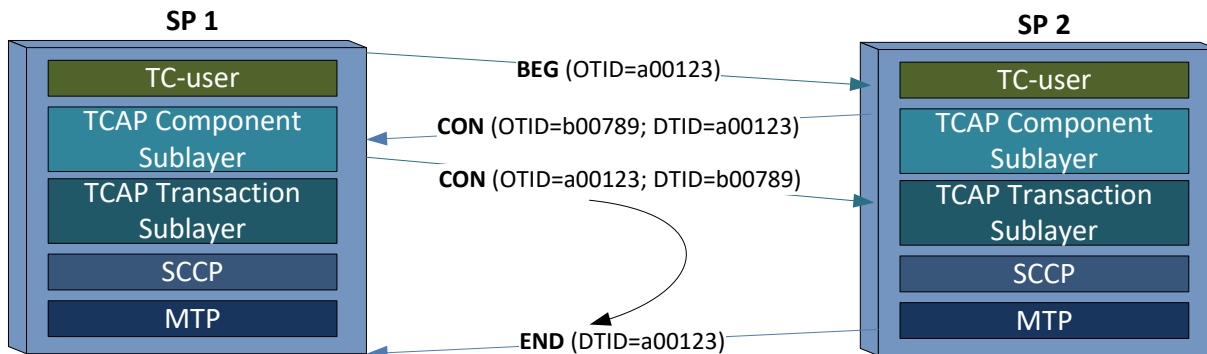


Figure A - 60. Structured TCAP Dialog example between Signaling Points.

#### A.3.3.3.2 TCAP Dialog Unit

Four APDU (Application Protocol Data Unit) are defined as part of the TCAP Dialog Portion:

- **Dialog Request** - APDU consisting of an application context name as well as, optionally, protocol version and user information. It is used to request dialog information to the other end such as the group of operations to include (context), as well as the discrimination of the protocol version to be used so as to avoid misinterpretations during the dialog. In other words, the «Dialog Request» may be interpreted as the agreed conversation language between TCAP ends.
- **Dialog Response** - APDU used for the response to a dialog start request. It includes the dialog request information elements, and additionally, result and diagnostic fields (in case of diagnosing a reject, the dialog is interrupted)

- **Dialog Abort** - APDU used for the termination of a dialog (related or not to the proposed protocol).
- **Dialog Unidirectional** - APDU consistent of an application context name as well as, optionally, protocol version and user information. Used for transmitting TCAP information to the other end, not expecting a response.

#### **A.3.3.3.2.1.1 Application Context Name**

The Application Context (AC) is a mechanism used by TCAP to identify the standard and the protocol version to be used within a transaction for a specific application layer, as several protocol versions exist for the available application layers (MAP/CAP/INAP, etc.). When a signaling entity receives a service invocation, it uses the AC name or ACN so as to determine which type of service is being invoked. In other words, when a service starts with TCAP BEGIN message, the ACN is included in the invocation request.

Each parameter of the ACN component is represented in TCAP by an octet.

The ACN embedded in the Dialog Unit represents an object identifier which essentially includes the following parameters:

- Regulatory Authority
- Organization
- Mobile Domain
- Mobile Subdomain
- AC Common Component Identifier
- Application Context
- Application Context Version

An ACN example extracted from a trace obtained by a protocol analyzer (Tektronix®) is shown next:

2.1.2.1.2 Application Context Name		
10100001	Tag	(CONT C [1])
00001001	Length	9
2.1.2.1.2.1 ACN Object ID		
00000110	Tag	(UNIV P Obj Identifier)
00000111	Length	7
0000	Authority	CCITT
- - - 0100	Organization	Identified-organization
00000000		ETSI
00000000	Domain	Mobile Domain
00000001	Mobile Subdomain	GSM / UMTS Network
00010101	Common Component ID	CAP 3 OE
00000011	CAP3 OE ID	ACE
00000100	Application Context	CAP-gsmSSF-SCF Generic

Another way of representing this identifier, according to ETSI specifications format, consistent with the upper example, is exhibited next:

{itu-t(0) identified-organization(4) etsi(0) mobileDomain(0) umts-network(1) cap3OE(21) ac(3) 4}.

#### A.3.3.3.2.1.2 Protocol Version

«Protocol Version» indicates the supported protocol version by the dialog unit. Thus, it assists to a correct understanding of the dialog information used between TC-users during the creation of new protocol versions within the dialog unit. This information is optional within the dialog unit.

#### A.3.3.3.2.1.3 User Info

«User Info» conveys information to be exchanged among TC-users only relevant for the application involved. It contains non-standardized parameters, which typically include the application layer operation code (MAP/CAP/INAP, etc.), parameters for numbering/origin/destination address, etc. This information is optional within the dialog unit.



#### **A.3.3.3.2.1.4 Result**

«Result» provides the dialog establishment result information to the originating TC-user.

#### **A.3.3.3.2.1.5 Result Resource Diagnostic**

«Result Source Diagnostic» identifies the origin of the result element and provides additional de diagnostic information.

#### **A.3.3.3.2.1.6 Abort Source**

«Abort Source» identifies the origin of an abnormal dialog termination, which may result in the TC-user or within the message dialog unit.

#### **A.3.3.3.2.1.7 Dialog Abort**

«Dialog Abort» is used to end a dialog beforehand its normal termination. It contains the termination origin information (user or service provider), and optionally, user information.

### **A.3.4 Mobile Application Part (MAP)**

MAP (Mobile Application Part), originally defined by ETSI and now specified by 3GPP TS 29.002, is currently widely deployed worldwide. It defines operations and procedures for the control y subscriber information presentation so as to enable messaging and roaming. The Global Title acquires a predominant role as long as the need for locating information outside of the subscriber's home network infrastructure/coverage or H-PLMN (Home Public Land Mobile Network).

MAP main functionalities include:

- *Mobility Services*: location management (for roaming support), authentication, subscriber information management, failure recovery.
- *Operation, Administration & Maintenance*: user tracking, subscriber's IMSI retrieval.
- *Call Management*: Routing, management during roaming, user state check for service authorization.
- *Supplementary Services (SS)*.
- *Messaging Services*: structured (SMS) and unstructured (USSD).
- *Packet Data Protocol (PDP) service for GPRS*: routing information delivery for GPRS connection establishment.
- *Location Services*: subscriber's geographic location retrieval.

#### **A.3.4.1 MAP Service Primitives and Dialogs**

MAP service primitives are named using the following notation:

*MAP-ServicePrimitiveName* type

where type may be one of the next types:

- request (req)
- indication (ind)
- response (rsp)
- confirm (cnf)

MAP services are then classified as:

- MAP provider unconfirmed-service
- MAP provider confirmed service (not necessarily by the other MAP user)
- MAP provider-initiated-service

MAP services are also distinguished as:

- Common MAP services
- MAP user specific services

MAP service primitives are encapsulated in the TCAP transaction portion of an SS7 MSU like depicted in next figure.

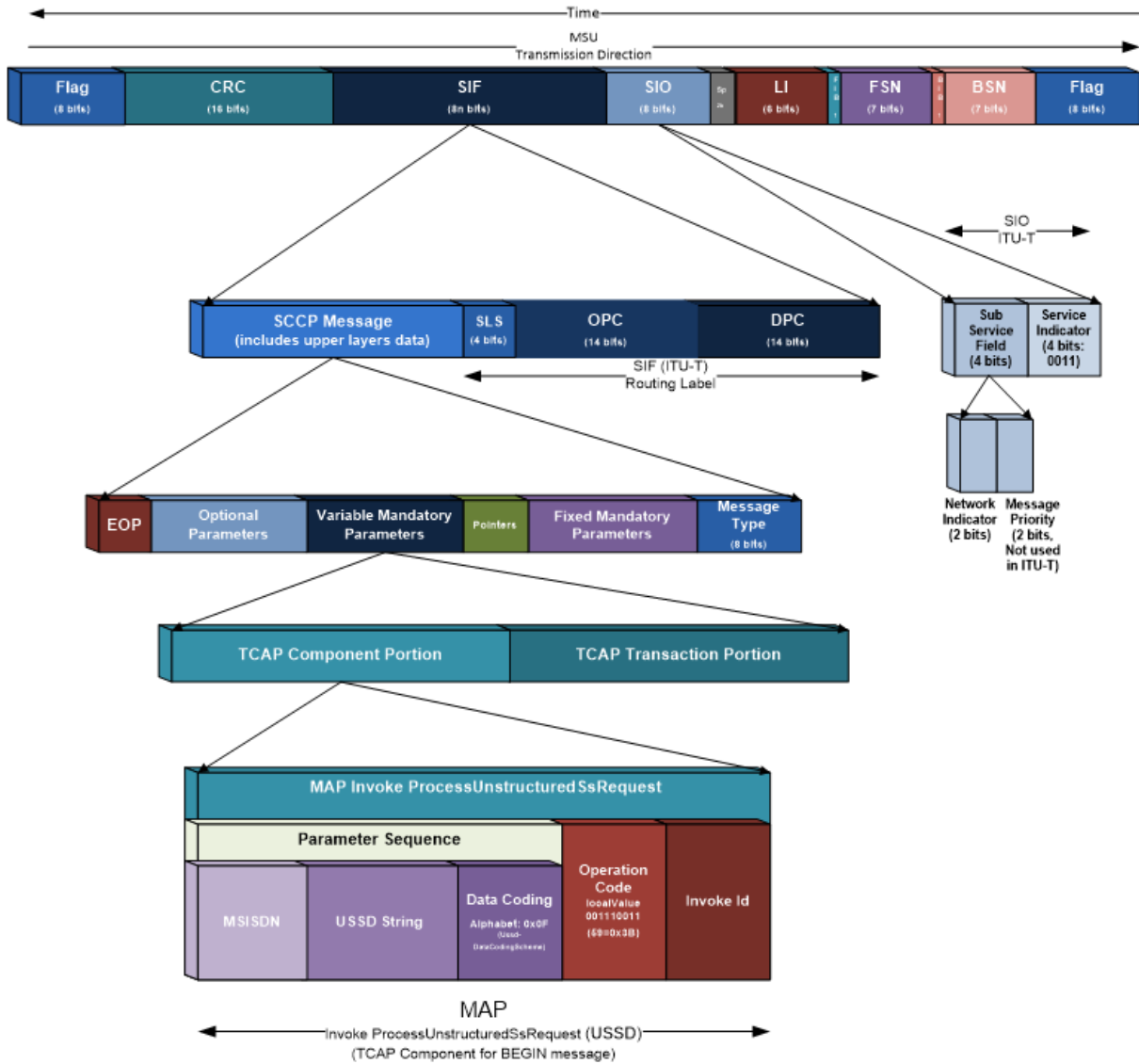


Figure A - 61. MAP service primitive (USSD) example embedded within an SS7 MSU.

A MAP dialog is defined as the needed information exchange between two MAP users to execute a specific task. A MAP dialog consists of one or several services. The dialog term derives from the TCAP vocabulary and adjusts to the data exchange between users of this layer.

Regarding data transfer among MAP, TCAP and an usufructuary application of these, GSM's structured dialog restriction simplifies the scenario. From TCAP's perspective, this demands a beginning with a BEGIN message, and the posterior ending with an END message if no errors occur. A special case is that which aborts a dialog through an ABORT message, which may be sent either by MAP or TCAP.

Every MAP service user requires access to services for the implementation of application layer basic functions:

- MAP dialog establishment and purge between MAP peers;
- Access lower layers' functions;
- Abnormal event reports;
- Different MAP versions management/compatibility;
- MAP dialog persistence check on the other end.

All MAP service primitives are listed next:

- **MAP-OPEN**: service used to initiate a dialog between two MAP users;
- **MAP-CLOSE**: service used to close a dialog between two MAP users;
- **MAP-DELIMITER**: service used to explicitly request MAP data unit transfer between peers;
- **MAP-U-ABORT**: service used to allow a MAP user request a MAP dialog abort;
- **MAP-P-ABORT**: service used to allow a MAP provider request a MAP dialog abort;
- **MAP-NOTICE**: service used to notify the MAP service provider to abort a MAP dialog due to protocol issues without affecting the protocol's state machine;

- **MAP-SECURE-TRANSPORT-CLASS-1:** confirmed service used for secure transport of a specific MAP service, which is mapped within a class 1 TCAP operation (e.g: an error result return);
- **MAP-SECURE-TRANSPORT-CLASS-2:** confirmed service used for secure transport of a specific MAP service, which is mapped within a class 2 TCAP operation (e.g: an error result return);
- **MAP-SECURE-TRANSPORT-CLASS-3:** confirmed service used for secure transport of a specific MAP service, which is mapped within a class 3 TCAP operation (e.g: an error result return);
- **MAP-SECURE-TRANSPORT-CLASS-4:** confirmed service used for secure transport of a specific MAP service, which is mapped within a class 4 TCAP operation (e.g: an error result return).

MAP-OPEN					MAP-DELIMITER				
Parameters	Request	Indication	Response	Confirm	Parameters	Request	Indication	Response	Confirm
Application Context Name	M	M (=)	U	C (=)	N/A				
Destination Address	M	M (=)			<b>MAP-NOTICE</b>				
Destination Reference	U	C (=)			Parameters	Request	Indication	Response	Confirm
Originating Address	U	O			Problem diagnostic	M			
Originating Reference	U	C (=)			<b>MAP-SECURE-TRANSPORT-CLASS-1</b>				
Specific Information	U	C (=)	U	C (=)	Parameters	Request	Indication	Response	Confirm
Responding Address			U	C (=)	Security header	M	M (=)	M	M (=)
Result			M	M (=)	Protected payload	C	C (=)	U	C (=)
Refuse-reason			C	C (=)	User error			U	C (=)
Provider error				O	Provider error				O
<b>MAP-CLOSE</b>					<b>MAP-SECURE-TRANSPORT-CLASS-2</b>				
Parameters	Request	Indication	Response	Confirm	Parameters	Request	Indication	Response	Confirm
Release Method	M				Security header	M	M (=)	M	M (=)
Specific Information	U	C (=)			Protected payload	C	C (=)		
					User error			U	C (=)
					Provider error				O

MAP-U-ABORT					MAP-SECURE-TRANSPORT-CLASS-3				
Parameters	Request	Indication	Response	Confirm	Parameters	Request	Indication	Response	Confirm
User reason	M	M (=)			Security header	M	M (=)	M	M (=)
Diagnostic information	U	C (=)			Protected payload	C	C (=)	U	C (=)
Specific information	U	C (=)			Provider error				O
MAP-P-ABORT					MAP-SECURE-TRANSPORT-CLASS-4				
Parameters	Request	Indication	Response	Confirm	Parameters	Request	Indication	Response	Confirm
Provider reason	M				Security header	M	M (=)		
Source	M				Protected payload	C	C (=)		

Table A - 14. Types and parameters for each MAP Service primitive.

### A.3.4.1.1 MAP Service Primitives' Sequence Rules

#### A.3.4.1.1.1 Opening

The MAP-OPEN service is invoked beforehand of any user-specific accepted service primitive. The sequence may or not contain one or several specific service primitives. In case of not containing neither of MAP-OPEN and MAP-DELIMITER service primitives, then an empty TCAP BEG message will be sent due to this condition. In case of including one or more specific service primitive, every one of them will be sent in the same TCAP BEG message. The sequence ends with a MAP-DELIMITER primitive.

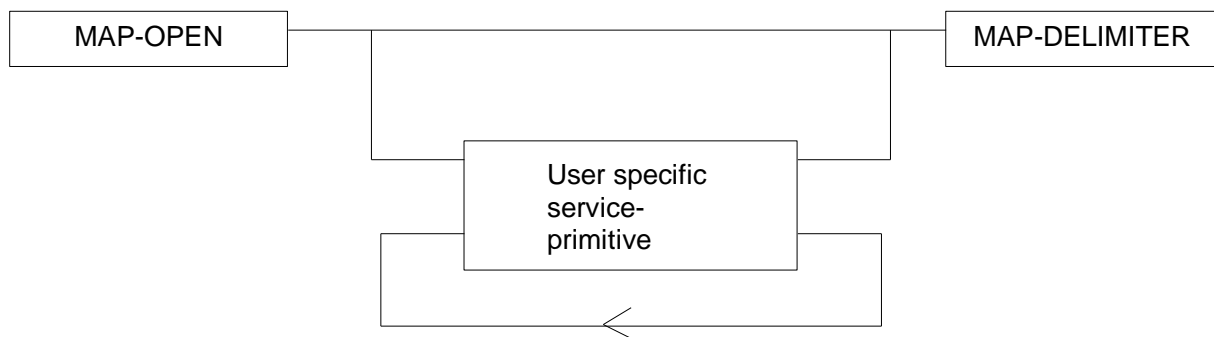


Figure A - 62. MAP Opening sequence.

**A.3.4.1.1.2 Continuing**

This sequence may or not be found present in some MAP dialogs. In case of existing, it ends with a MAP-DELIMITER primitive. If more than one specific service primitive is included, every one of them are included TCAP CON message.

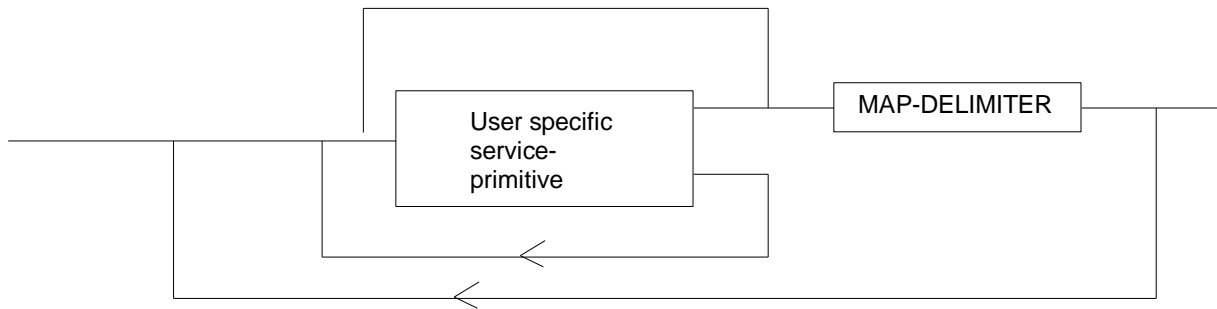


Figure A - 63. MAP Continuing sequence.

**A.3.4.1.1.3 Closing**

This sequence may only appear after an Opening or Continuing sequence. The sequence may or not contain one or several specific service primitives if the MAP-CLOSE primitive specifies a normal release. In case of not including a specific service primitive, then an empty TCAP BEG message will be sent due to this condition. In case of including several service primitives, every one of them will be sent in the same TCAP END message. In case of presetting an END message, the sequence cannot contain any specific service primitive. MAP-CLOSE primitive must be sent after the delivery of all specific service primitives of all MAP services provider users.

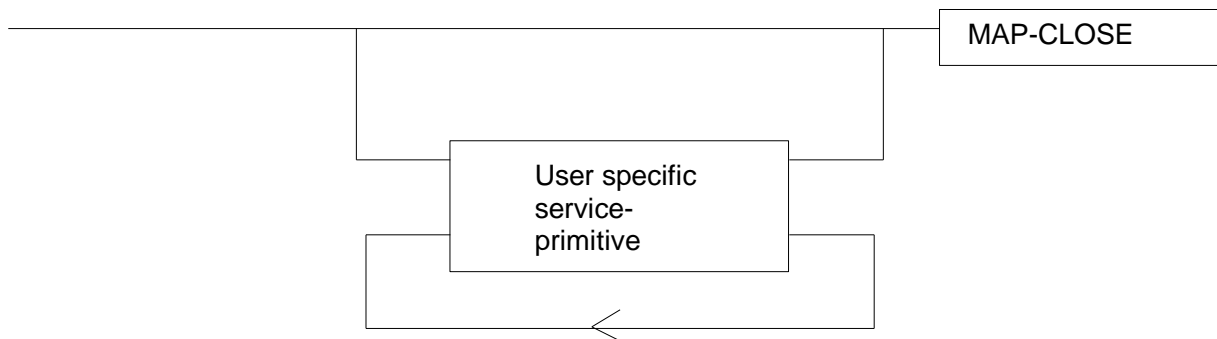


Figure A - 64. MAP Closing sequence.

#### A.3.4.1.1.4 Aborting

A MAP service user may use a MAP-U-ABORT service primitive at any moment after the opening of a MAP dialog or as a response to a MAP dialog opening attempt.



Figure A - 65. MAP Aborting sequence.

The MAP service provider may use MAP-P-ABORT service primitive towards a MAP service user for which there is an open MAP dialog.

MAP-U-ABORT and/or MAP-P-ABORT service primitives end a MAP dialog.

In case of receiving a “resource unavailable (short term problem)” as termination reason within a MAP-U-ABORT service primitive, the MAP user service may retry establishing a new MAP dialog immediately.

#### A.3.4.1.1.5 General rules for mapping of MAP services onto TCAP

Next Table provides an overview of the mapping rules for mapping of common services onto TC-services.

MAP service-primitive	TC service-primitive
MAP-OPEN request (+ any user specific service primitives) + MAP-DELIMITER request	TC-BEGIN request (+ component handling primitives)
MAP-OPEN response (+ any user specific service primitives) + MAP-DELIMITER request	TC-CONTINUE request (note) (+ component handling primitives)
(any user specific service primitives)	TC-CONTINUE request



+ MAP-DELIMITER request	(+ component handling primitives)
(any user specific service primitives) + MAP-CLOSE request	TC-END request (+ component handling primitives)
MAP-U-ABORT request	TC-U-ABORT request
NOTE: or TC-END if the MAP-CLOSE request has been received before the MAP-DELIMITER request.	

Table A - 15. Mapping of MAP common services onto TCAP services [22].

Next Table provides the mapping rules for mapping of TC-services onto common services.

TC service-primitive	MAP service-primitive
TC-BEGIN indication (+ component handling primitives)	MAP-OPEN indication (+ user specific service primitives) + MAP-DELIMITER indication (note 1)
TC-CONTINUE indication (+ component handling primitives)	First time: MAP-OPEN confirm (+ user specific service primitives) + MAP-DELIMITER indication (note 1)  Subsequent times: (user specific service primitives) + MAP-DELIMITER indication (note 1)
TC-END indication (+ component handling primitives)	MAP-OPEN confirm (note 6) (user specific service primitives) + MAP-CLOSE indication
TC-U-ABORT indication	MAP-U-ABORT indication or MAP-P-ABORT indication (note 2) MAP-OPEN confirmation (note 3)
TC-P-ABORT indication	MAP-P-ABORT indication (note 4) MAP-OPEN confirmation (note 5)
NOTE 1: It may not be necessary to present this primitive to the user for MAP	

version 2 applications.

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

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

NOTE 4: If the "Abort Reason" in the TC-P-ABORT indication is set to a value different from "Incorrect Transaction Portion".

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

NOTE 6: Only if opening sequence is pending.

Table A - 16. Mapping of TC services onto MAP common service [22].

Next Table provides the general mapping rules which apply to mapping of MAP user specific services onto TC services.

<b>MAP service-primitive</b>	<b>TC-service-primitive</b>
MAP-xx request	TC-INVOKE request
MAP-xx response (note 1)	TC-RESULT-L request TC-U-ERROR request TC-U-REJECT request TC-INVOKE request (note 2)
NOTE 1: The mapping is determined by parameters contained in the MAP-xx response primitive.	
NOTE 2: This applies only to TC class 4 operations where the operation is used to pass a result of another class 2 or class 4 operation.	

Table A - 17. Mapping of MAP user specific services onto TC services [22].

Next Table provides the general mapping rules for mapping of TC services onto MAP user specific services.

<b>TC-service-primitive</b>	<b>MAP service-primitive</b>
TC-INVOKE indication	MAP-xx indication
TC-RESULT-L indication (note 4) TC-U-ERROR indication TC-INVOKE indication (note 2) TC-L-CANCEL indication	MAP-xx confirm
TC-U-REJECT indication TC-L-REJECT indication TC-R-REJECT indication	MAP-xx confirm or MAP-NOTICE indication (note 3)
NOTE 1: The mapping is determined by parameters contained in the MAP-xx response primitive.	
NOTE 2: This applies only to TC class 4 operations where the operation is used to pass a result of another class 2 or class 4 operation.	
NOTE 3: The detailed mapping rules are given in clause 16.	
NOTE 4: If RESULT-NL components are present they are mapped onto the same MAP-xx confirm	

Table A - 18. Mapping of TC services onto MAP user specific services [22].

#### **A.3.4.1.1.6 MAP Service primitives' parameters**

##### **A.3.4.1.1.6.1 Invoke Id**

The «Invoke Id» parameter identifies MAP service primitives. This parameter is supplied by the MAP service user and must be unique over each user/provider interface.

For instance, when requesting location parameters to the HLR (MAP ATI operation), the Invoke Id is identical either for invocation and response, i.e., for TCAP Invoke and Return\_Result\_Last transaction components (common rule for structured MAP services). Another classic example of this rule is the one applying for MAP Short Message Service (SMS) also for TCAP Invoke and Return\_Result\_Last transaction components.

This rule does not apply in unstructured MAP services such as USSD. Within a USSD session, multiple identifiers may be used on each instance. It's of crucial importance noting that for each component type an identifier must then be entered following the same criteria. During an iterated transaction such as USSD, the Invoke ID parameter is increased since the first service invocation.

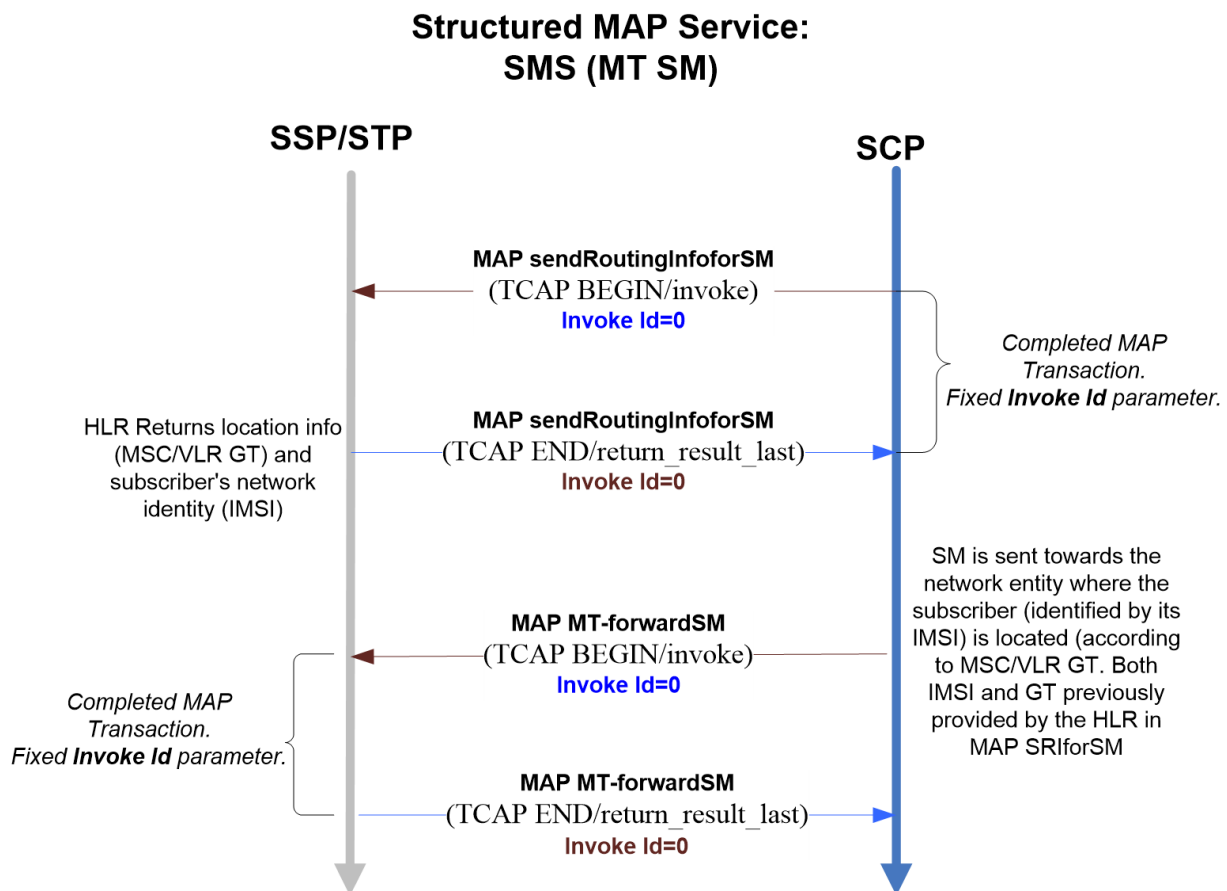


Figure A - 66. Structured MAP service (SMS) «Invoke Id» values example.

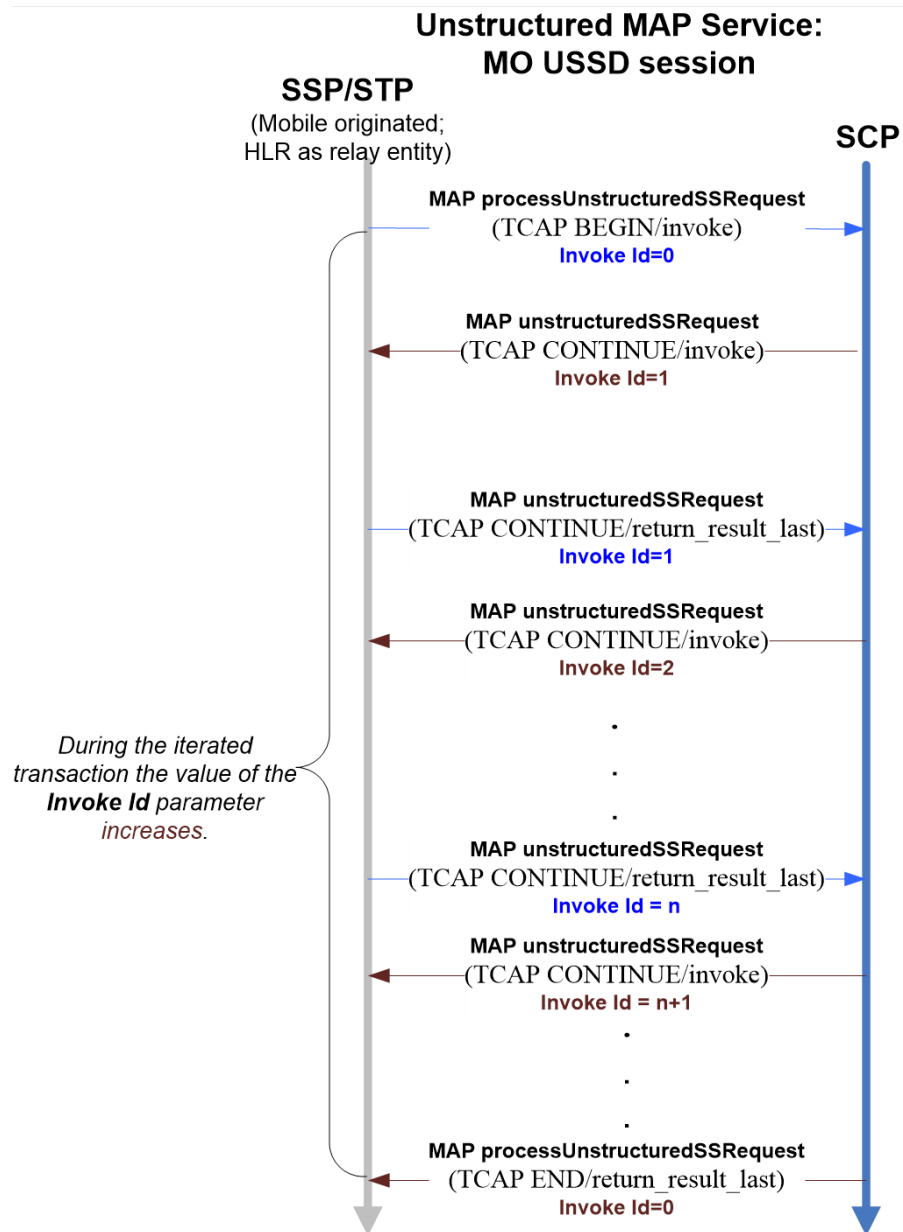


Figure A - 67. Unstructured MAP service (USSD) «Invoke Id» values example.

**A.3.4.1.1.6.2 Linked Id**

The «Linked Id» parameter is used for linked services seizing their Invoke Id parameter value.

#### **A.3.4.1.1.6.3 Provider Error**

The «Provider error» parameter is used to indicating a type of protocol/provider error, namely:

- Duplicated Invoke Id.
- Unsupported service.
- Invalid parameter syntax.
- Resource limit.
- Ongoing dialog release.
- Unexpected response from the peer user.
- Service completion failure.
- Response absence from the pair user.
- Invalid response reception.

#### **A.3.4.1.1.6.4 User Error**

The «User error» parameter indicates an error associated to a MAP user action, namely:

- Generic error.
- Numbering or identification error.
- Subscription error.
- Overlap or handover error.
- Operation and maintenance error.
- Call establishment error.
- Supplementary service error.
- Short message service error.
- Location services error.
- Error detected by an application using secured transport.

#### **A.3.4.1.1.6.5 Operation Codes**

A TCAP/MAP component message possesses a numeric operation code or «Operation Code» which identifies the exchanged information of a particular service.

The following table lists the MAP operation codes and its values, groups by type of operations. The ACN for each operation is also provided.

MAP Operation	Operation Code (Bin   Decimal   Hexa)			Application Context Name
<b>Location Registration Operations</b>				
<b>UpdateLocation</b>	00000010	2	2	networkLocUpContext
<b>CancelLocation</b>	00000011	3	3	locationCancellationContext
<b>PurgeMS</b>	01000011	67	43	msPurgingContext
<b>SendIdentification</b>	00110111	55	37	interVlrInfoRetrievalContext
<b>GPRS Location Registration Operations</b>				
<b>UpdateGprsLocation</b>	00010111	23	17	gprsLocationUpdateContext
<b>Subscriber Information Enquiry Operations</b>				
<b>ProvideSubscriberInfo</b>	01000110	70	46	subscriberInfoEnquiryContext
<b>Any Time Information Enquiry Operations</b>				
<b>AnyTimeInterrogation</b>	01000111	71	47	anyTimeInfoEnquiryContext
<b>Authentication Management Operations</b>				
<b>SendAuthenticationInfo</b>	00111000	56	38	infoRetrievalContext
<b>AuthenticationFailureReport</b>	00001111	15	F	authenticationFailureReportContext
<b>IMEI Management Operations</b>				
<b>CheckIMEI</b>	00101011	43	2B	equipmentMngtContext
<b>Subscriber Management Operations</b>				
<b>SendParameters</b>	00001001	9	9	infoRetrievalContext
<b>InsertSubscriberData</b>	00000111	7	7	networkLocUpContext gprsLocationUpdateContext subscriberDataMngtContext
<b>DeleteSubscriberData</b>	00001000	8	8	subscriberDataMngtContext
<b>Fault Recovery Management Operations</b>				

<b>Reset</b>	00100101	37	25	resetContext
<b>ForwardChecksIndication</b>	00100110	38	26	networkLocUpContext
<b>RestoreData</b>	00111001	57	39	
<b>Any Time Information Handling Operations</b>				
<b>PerformHandover</b>	00011100	28	1C	handoverControlContext
<b>PrepareHandover</b>	01000100	68	44	
<b>SendEndSignal</b>	00011101	29	1D	
<b>ProcessAccessSignaling</b>	00100010	34	22	
<b>ForwardAccessSignaling</b>	00100010	34	22	
<b>PerformSubsequentHandover</b>	00011110	30	1E	
<b>PrepareSubsequentHandover</b>	01000101	69	45	
<b>GPRS Location Information Retrieval Operations</b>				
<b>SendRoutingInfoForGprs</b>	00011000	24	18	gprsLocationInfoRetrievalContext
<b>Failure Reporting Operations</b>				
<b>FailureReport</b>	00011001	25	19	failureReportContext
<b>GPRS Notification Operations</b>				
<b>NoteMsPresentForGprs</b>	00011010	26	1A	gprsNotifyContext
<b>Mobility Management Operations</b>				
<b>NoteMmEvent</b>	01011001	89	59	mm-EventReportingContext



Operation and Maintenance Operations				
<b>ActivateTraceMode</b>	0 0 1 1 0 0 1 0	50	32	tracingContext networkLocUpContext gprsLocationUpdateContext
<b>DeactivateTraceMode</b>	0 0 1 1 0 0 1 1	51	33	tracingContext
<b>TraceSubscriberActivity</b>	0 1 0 1 0 0 1 0	82	52	handoverControlContext
<b>NoteInternalHandover</b>	0 0 1 1 0 1 0 1	53	35	
<b>SendIMSI</b>	0 0 1 1 1 0 1 0	58	3A	imsiRetrievalContext
<b>ReleaseResources</b>	0 0 0 1 0 1 0 0	20	14	resourceManagementContext
Call Handling Operations				
<b>SendRoutingInfo</b>	0 0 0 1 0 1 1 0	22	16	locationInfoRetrievalContext
<b>ProvideRoamingNumber</b>	0 0 0 0 0 1 0 0	4	4	roamingNumberEnquiryContext
<b>ResumeCallHandling</b>	0 0 0 0 0 1 1 0	6	6	callControlTransferContext
<b>ProvideSIWFSNumber</b>	0 0 0 1 1 1 1 1	31	1F	siWFSAllocationContext
<b>Siwfs-signalingModify</b>	0 0 1 0 0 0 0 0	32	20	siWFSAllocationContext
<b>SetReportingState</b>	0 1 0 0 1 0 0 1	73	49	reportingContext
<b>StatusReport</b>	0 1 0 0 1 0 1 0	74	4A	
<b>RemoteUserFree</b>	0 1 0 0 1 0 1 1	75	4B	
<b>Ist-Alert</b>	0 1 0 1 0 1 1 1	87	57	istAlertingContext
<b>Ist-Command</b>	0 1 0 1 1 0 0 0	88	58	ServiceTerminationContext

<b>Group Call Operations</b>				
<b>PrepareGroupCall</b>	00100111	39	27	groupCallControlContext
<b>SendGroupCallEndSignal</b>	00101000	40	28	
<b>ProcessGroupCallSignaling</b>	00101001	41	29	
<b>ForwardGroupCallSignaling</b>	00101010	42	2A	
<b>SendGroupCallInfo</b>	01010100	84	54	groupCallInfoRetrievalContext
<b>Supplementary Service Operations</b>				
<b>RegisterSS</b>	00001010	10	A	networkFunctionalSsContext
<b>EraseSS</b>	00001011	11	B	
<b>ActivateSS</b>	00001100	12	C	
<b>DeactivateSS</b>	00001101	13	D	
<b>InterrogateSS</b>	00001110	14	E	
<b>ProcessUnstructuredSsData</b>	00011001	25	19	
<b>ProcessUnstructuredSsRequest</b>	00111011	59	3B	networkUnstructuredSsContext
<b>UnstructuredSsRequest</b>	00111100	60	3C	
<b>UnstructuredSsNotify</b>	00111101	61	3D	
<b>RegisterPassword</b>	00010001	17	11	networkFunctionalSsContext
<b>GetPassword</b>	00010010	18	12	
<b>BeginSubscriberActivity</b>	01010100	84	54	

<b>SsInvocationNotification</b>	01001000	72	48	ss-InvocationNotificationContext
<b>Short Message Service Operations</b>				
<b>SendRoutingInfoForSM</b>	00101101	45	2D	shortMsgGatewayContext
<b>MO-ForwardSM</b>	00101110	46	2E	shortMsgMO-RelayContext
<b>MT-ForwardSM</b>	00101100	44	2C	shortMsgMT-RelayContext
<b>ReportSmDeliveryStatus</b>	00101111	45	2D	shortMsgGatewayContext
<b>NoteSubscriberPresent</b>	01001000	36	24	mwdMngtContext
<b>AlertServiceCentreWithoutResult</b>	01001001	73	49	shortMsgAlertContext
<b>AlertServiceCentre</b>	01000000	64	40	
<b>InformServiceCentre</b>	00111111	63	3F	shortMsgGatewayContext
<b>ReadyForSM</b>	01000010	64	40	mwdMngtContext

Table A - 19. MAP Operation Codes and Application Context Names.

### A.3.5 Customised Applications for Mobile Enhanced Logic (CAMEL)

CAMEL (Customised Applications for Mobile Enhanced Logic) Project, specified in 3GPP TS 23.078 and CAP (CAMEL Application Part, 3GPP TS 29.078) protocol, comprise an INAP evolution towards global mobility. According to 3GPP TS 23.078 (from CAMEL Phase 4; Stage 2), the following type of operations are defined as part of the CAMEL concept are defined, among others:

- Circuit Switched Call Control;
- GPRS Session Control / GPRS Interworking;
- SMS Control;
- USSD session from/to the gsmSCF at the SCP;
- Supplementary Services notification;
- Mobility Management;
- Control/Query/Modification of CAMEL Subscription Information (CSI);
- Subscriber Location information and State retrieval;
- Mobile Number Portability (MNP).

During the 1990's, INAP (Intelligent Network Application Protocol) was the dominant protocol among Intelligent Networks (IN), whom satisfactorily operated within fixed private networks. However, two aspects became issues to fix:

- Lack of standard developments from manufacturers became a problem, mainly due to voids in the specification.
- No mobility.

Meanwhile GSM became the dominant system among mobile networks, users became able to access services in foreign mobile networks. These obliged carriers to provide services to users while roaming. For this purpose, ETSI started the CAMEL (Customized Applications for Mobile Enhanced Logic) project by late 1995 (today specified by 3GPP TS 23.078, phase IV). CAP (CAMEL Application Part) emerges, which could be established as INAP evolution towards global mobility.

CAP is currently specified by 3GPP TS 29.078. Several services are implemented under CAP, being its main competencies:

- CAMEL Call Control (from CAMEL Phase II)
- CAMEL Control of GPRS (from CAMEL Phase III)
- CAMEL Control of SMS (from CAMEL Phase III)

One of CAMEL major abilities comprises the implementation of the IN control used between the gsmSSF and the gsmSCF.

CAP capabilities are defined through “operations”, which can be demarcated as a mechanism by which an entity initiates a procedure in a peer. A classic example is the delivery of an IDP (Initial Detection Point) operation by a gsmSSF within an MSC (SSP) towards a gsmSCF of an SCP so as to invoking a CAMEL service. The SCP can send a response back, initiating one or more procedures at the gsmSSF. This response delivery depends on the specific operation and the process result of such operation.

CAMEL’s advent modified the terminology, interfaces and communication protocols between network entities as compared to how IN was being driven. The functions of network entities of a PLMN (Public Land Mobile Network) defined for CAMEL are listed next.

- GSM Service Control Function (gsmSCF): functional entity that contains the CAMEL service logic to implement Operator Specific Service. The Service Control Point (SCP) encompasses the service logic codes through the gsmSCF, which handles CAMEL service procedures as well as user or network information through the Service Data Function (SDF).

An SSP provides IN functionalities access. It contains a Switch Call Control Function (CCF) providing call/service processing and control as specified by ITU-T Q.1224, and a Service Switching Function (SSF) which interacts with the SCF. MSC (Mobile Switching Centre) and GMSC (Gateway MSC) contains SSP capabilities for CAMEL compliance in Circuit-Switched Core Networks, while SGSN (Serving GPRS Support Node) does within Packet-Switched Core Networks. SSF entities are listed next:

- GSM Service Switching Function (gsmSSF): functional entity that interfaces the MSC or GMSC to the gsmSCF. The concept of the gsmSSF is derived from the IN SSF, but uses different triggering mechanisms because of the nature of the mobile network.
- GPRS Service Switching Function (gprsSSF): functional entity that interfaces the SGSN (Serving GPRS Support Node) to the gsmSCF. The concept of the gprsSSF is derived from the IN SSF, but uses different triggering mechanisms because of the nature of the mobile network.
- Short Message Service Service Switching Function (smsSSF): functional entity that interfaces the MSC or SGSN to the gsmSCF for Short Message Service.

Other CAMEL functions are listed next:

- GSM Specialized Resource Function (gsmSRF). An MSC or GMSC may contain a GSM Specialized Resource Function (gsmSRF). A gsmSRF provides subscriber interaction capability. A gsmSCF may use an established CAMEL relationship with an MSC or GMSC to instruct the gsmSSF to connect a call to the gsmSRF and then instruct the gsmSSF to apply user interaction (e.g. to play an announcement).
- Intelligent Peripheral (IP) or Specialized Resource Point (SRP) - (gsmSRF). An IP or SRP offers similar user interaction capability as an MSC/assisting gsmSSF. An IP is however a stand-alone node, dedicated to offering user interaction. RBT (Ring Back Tone) or voice-menu driven pre-paid voucher top up are typical services of IP or SRP.
- Short Message Service Centre (SMSC). This entity could be divided in two main modules, the SMS IWMSC (Inter Working MSC) and the SC (Service Centre). The SMSC interacts through MAP with the MSC, SGSN and the HLR.
- Gateway Mobile Location Centre (GMLC). This entity allows external Location Service Clients to request real-time location information of a Mobile Station.

- Serving Mobile Location Centre (SMLC). Functional entity that performs location information retrieval from the Radio Access Network.
- Mobile Number Portability Signaling Relay Function (MNP SRF). Functional entity that supports the mobile number portability of a mobile station, which is described in 3GPP TS 23.066

The following interfaces are defined for CAMEL:

- HLR - VLR. Interface Used to send the CAMEL related subscriber data to the visited PLMN and for provision of MSRN (Mobile Subscriber Roaming Number). The interface is also used to retrieve mobile subscriber status and location information or to indicate suppression of announcement for a CAMEL service.
- GMSC – HLR. Interface used at terminating calls to exchange routing information, subscriber status, location information, subscription information and suppression of announcements. The CAMEL related subscriber data that is passed to the IPLMN is sent over this interface.
- GMSC – gsmSSF. This is an internal interface used for handling of Detection Points (arming/disarming of DPs, DP processing etc.).
- gsmSSF – gsmSCF. Interface used by the gsmSCF to control a call in a certain gsmSSF and to request the gsmSSF to establish a connection with a gsmSRF. Relationships on this interface are opened as a result of the gsmSSF sending a request for instructions to the gsmSCF or opened as a result of the gsmSCF sending a request to the gsmSSF to initiate a new call.
- MSC – gsmSSF. This is an internal interface used for handling of DPs (arming/disarming of DPs, DP processing etc.).
- gsmSCF - HLR. This interface is used by the gsmSCF to request information from the HLR. As a network operator option the HLR may refuse to provide the information requested by the gsmSCF.

- gsmSCF – gsmSRF. This interface is used by the gsmSCF to instruct the gsmSRF to play tones/announcements to the users.
- GMSC – MSC. This interface is used to transfer control of a call from a VMSC back to a GMSC for optimal routing.

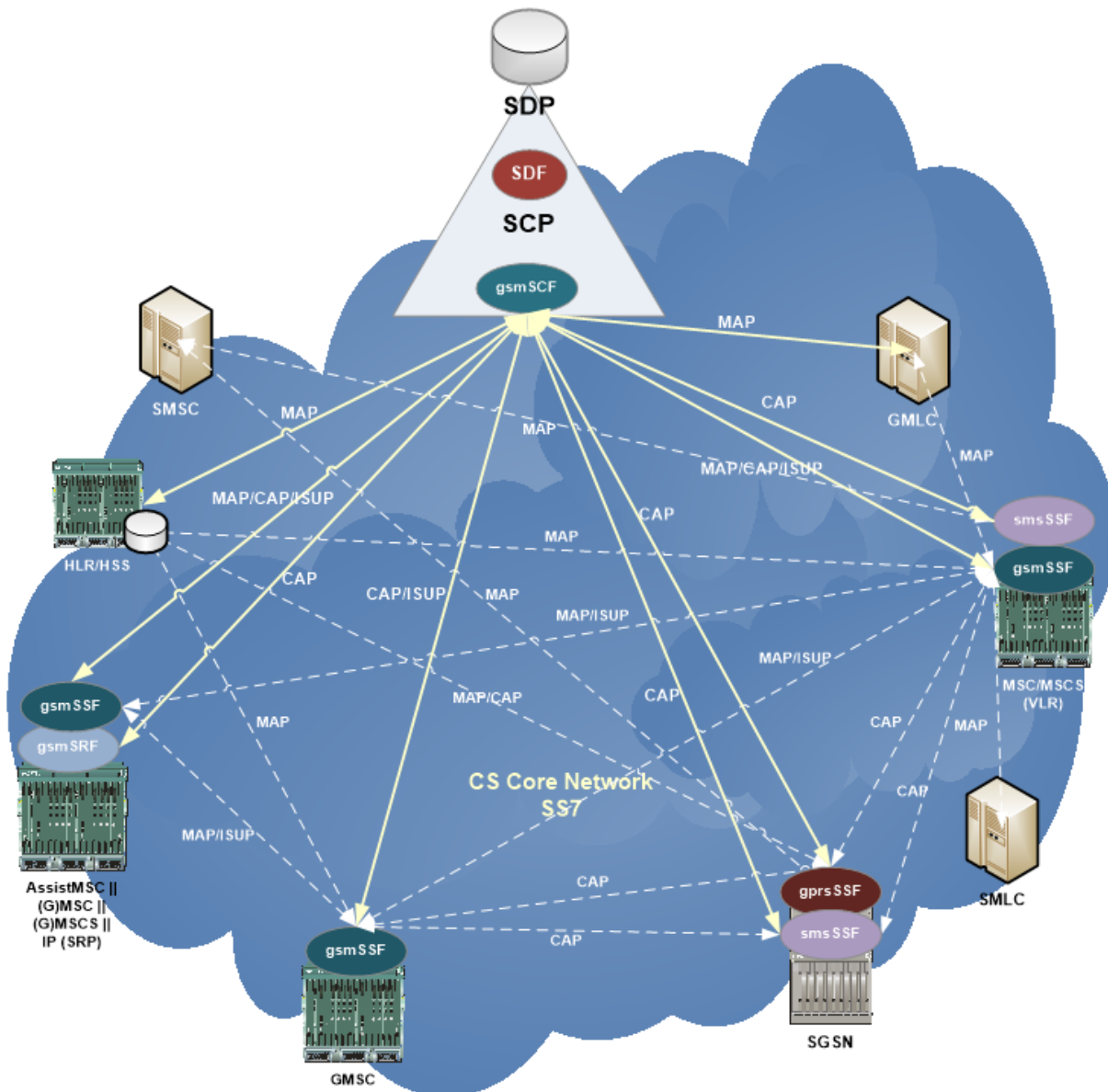


Figure A - 68. CAMEL functions, entities/nodes and interfaces in SS7 based Core Networks.



Some classic CAMEL services examples are detailed next:

- Calling Name Presentation: comprises the ability of presenting the name of originating party of the call to the called party (using a query database instead of forcing a handset setup in this sense).
- Prepay and Account Spending Limit (ASL): allow use measuring either for prepaid or postpaid subscribers, so as to providing them a way of control of their expenses. Some markets include parent control, corporative resource allocation, etc.
- Incoming Call Management (ICM): allows automatic incoming call management, so as to providing management means to the user. Examples: route all calls to voice mail except those from a list of priority numbers; route all calls to a specific mobile number during a specific time span; etc.
- Virtual Private Network (VPN): CAMEL allows replicating PBX scenario within mobile telephony. VPN comprise then corporative subscriber call manager platforms, where functionalities like the following are implemented: White/Black Lists; Call Scheduling; Extension Number White/Black Lists; Onnet/Offnet Corporative Tariff Table; Abbreviated Dialing / Short Codes; Frequent Numbers; Emergency Calls; etc.
- Call Redirect Services (CRS): CAMEL provides redirect services to user while roaming like its native Customer Care (\*611).
- Location Based Services (LBS): these applications trust on CAMEL for location information search engines, user directory, emergency service, information exchange among distributed databases, assistance to a Public Service Answering Point (PSAP), LBS infrastructure like Gateway Mobile Location Centre (GMLC) and Serving Mobile Location Centre (SMLC) queries for Assisted-GPS or OTDOA (Observed Time Difference of Arrival) precise location information retrieval, etc.

### A.3.5.1 CAP Definitions and Architecture

CAP protocol definition may be divided in three sections:

- Protocol definition rules for SACF/MACF (Single Association Control Function / Multiple Association Control Function).
- Definition of operations (according to ASN.1) transferred among the network entities.
- Definition of the executed actions at each entity (in terms of state transition diagrams).

CAP comprises a ROSE (Remote Operations Service Element) type user protocol, embedded inside component sublayer.

Rules to be applied by SACF/MACF are described next:

➤ Reflection of TCAP Application Context

- TC AC negotiation rules require that the proposed AC, if acceptable, is reflected in the first backwards message.
- If the gsmSSF, gprsSSF or smsSSF provides an AC which is not acceptable to the gsmSCF, then an alternate AC shall not be returned. If the AC presented to the gsmSCF is not acceptable, then this is most probably due to an error in subscriber data provisioning or an error at the gsmSSF, gprsSSF or smsSSF.

➤ Sequential/parallel execution of operations

In some cases, it may be necessary to distinguish whether operations should be performed sequentially or in parallel (synchronised). Operations which may be synchronised are:

- Charging operations; may be synchronised with any other operation(s).

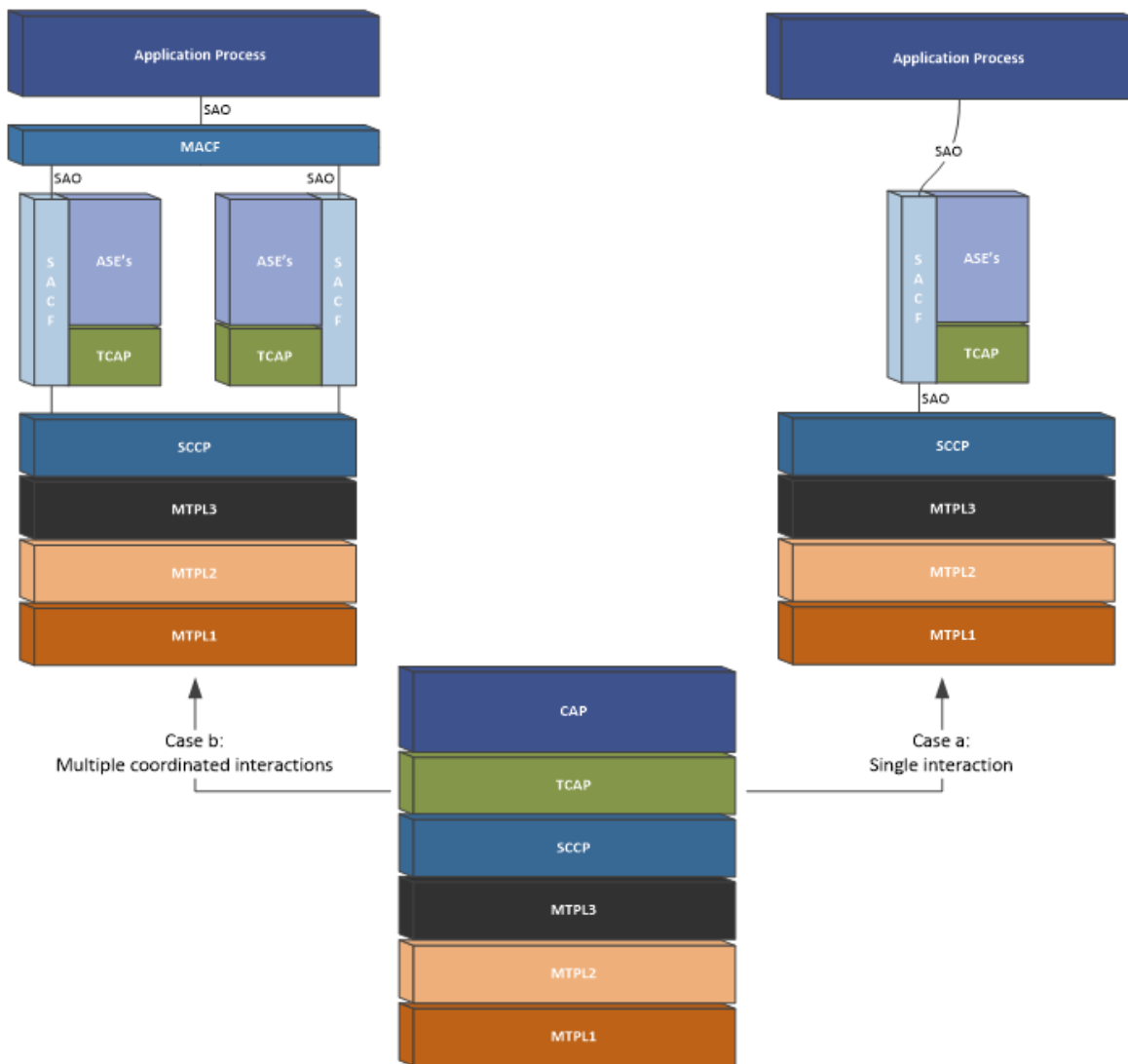


Figure A - 69. CAP protocol architecture.

The method of indicating to the receiving entity that operations should be synchronised is by transmitting these operations within a single TC message. If one of the operations identified above shall not be executed until the execution of another operation has progressed to a certain extent or has finished, then the sending PE shall control this by sending the operations in two separate TC messages. This method does not imply that all operations sent in a single TC message shall be executed simultaneously, but that where it could make sense to do so (in the situations identified above) the operations should be synchronised. In the case of inconsistency between the above-mentioned generic rules and the FE-specific rules, the FE-specific rules take precedence over the generic rules.

CAP is derived from Core INAP CS1/2. One of CAMEL's utmost capabilities include the implementation of IN control protocol used between the gsmSSF and the gsmSCF. CAP capabilities are defined through "operations", which can be demarcated as a mechanism by which an entity initiates a procedure in a peer. A classic example is the delivery of an IDP (Initial Detection Point) operation by a gsmSSF within an MSC (SSP) towards a gsmSCF of an SCP so as to invoking a CAMEL service. The SCP can send a response back, initiating one or more procedures at the gsmSSF. This response delivery depends on the specific operation and the process result of such operation.

Three types of information can be specified for each operation:

- Argument – The originating entity can include arguments in an operation. Arguments comprise parameters as inputs for CAMEL service processing.
- Result – A result is defined for some operations. The receiver of an operation can report the processing result in this field.
- Errors – The receiver can return an error as result of an operation processing. After a time determined for each CAP operation, in case of not receiving an error report, the originating entity will consider it as satisfactory.

#### A.3.5.1.1 CAP Operations

Next table exhibits all CAP operations defined for CAMEL Call, SMS and GPRS control.

Operation	Acronym	CAP Operation Packages	Op. Code (Dec)	Op. Code (Hex)	ACN CAP3OE UMTS	ACN CAP4 UMTS	ACN CAP4OE UMTS
<b>CAP Operations for Call Control</b>							
<b>initialDP</b>	<b>IDP</b>	gsmSCF activation Package [0]	0	0	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>assistRequestInstructions</b>	<b>ARI</b>	gsmSCF/gsmSRF activation of	16	10	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)

		assist Package [15]					
<b>establishTemporaryConnection</b>	<b>ETC</b>	Assist connection establishment Package [16]	17	11	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>disconnectForwardConnection</b>	<b>DFC</b>	Generic disconnect resource Package [17]	18	12	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>dFCWithArgument</b>	<b>DFCWA</b>		86	56	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>connectToResource</b>	<b>CTR</b>	Non-assisted connection establishment Package [18]	19	13	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>Connect</b>	<b>CON</b>	Connect Package (elementary gsmSSF function) [19]	20	14	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>releaseCall</b>	<b>RC</b>	Call handling Package (elementary gsmSSF function) [20]	22	16	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>requestReportBCSMEvent</b>	<b>RRB</b>	BCSM Event handling Package [21]	23	17	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>eventReportBCSM</b>	<b>ERB</b>		24	18	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>Continue</b>	<b>CUE</b>	gsmSSF call processing Package [24]	31	1F	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>initiateCallAttempt</b>	<b>ICA</b>	gsmSCF call initiation Package [25]	32	20	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>resetTimer</b>	<b>RT</b>	Timer Package [26]	33	21	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>furnishChargingInformation</b>	<b>FCI</b>	Billing Package [27]	34	22	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>applyCharging</b>	<b>ACH</b>	Charging Package [28]	35	23	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)
<b>applyChargingReport</b>	<b>ACR</b>		36	24	04 00 1 21 3 (4)	04 00 1 22 3 (4)	04 00 1 23 3 (4)

<b>callGap</b>	<b>CG</b>	Traffic management Package [29]	41	29	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>callInformationReport</b>	<b>CIRp</b>	Call report Package [32]	44	2C	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>callInformationRequest</b>	<b>CIRq</b>		45	2D	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>sendChargingInformation</b>	<b>SCI</b>	signaling control Package [33]	46	2E	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>playAnnouncement</b>	<b>PA</b>	Specialized resource control Package [42]	47	2F	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>promptAndCollectUserInfo</b>	<b>PC</b>		48	30	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>specializedResourceReport</b>	<b>SRR</b>		49	31	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>Cancel</b>	<b>CAN</b>	Cancel Package [36]	53	35	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>activityTest</b>	<b>AT</b>	Activity Test Package [34]	55	37	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>continueWithArgument</b>	<b>CWA</b>	CPH Response Package [37]	88	58	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>disconnectLeg</b>	<b>DL</b>		90	5A	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>moveLeg</b>	<b>ML</b>		93	5D	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>splitLeg</b>	<b>SL</b>		95	5F	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>entityReleased</b>	<b>EL</b>	Exception Inform Package [38]	96	60	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>playTone</b>	<b>PT</b>	Play Tone Package [39]	97	61	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>CAP Operations for GPRS Control</b>							
<b>activityTestGPRS</b>	<b>AT GPRS</b>	Gprs Activity Test Package [58]	70	46	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>applyChargingGPRS</b>	<b>ACH GPRS</b>	Gprs Charging Package [57]	71	47	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>applyChargingReportGPRS</b>	<b>ACR GPRS</b>		72	48	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)

cancelGPRS	<b>CAN GPRS</b>	Gprs Cancel Package [59]	73	49	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
connectGPRS	<b>CON GPRS</b>	Gprs Connect Package [52]	74	4A	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
continueGPRS	<b>CUE GPRS</b>	Gprs Continue Package [49]	75	4B	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
entityReleasedGPRS	<b>ER GPRS</b>	Gprs Exception Information Package [50]	76	4C	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
furnishChargingInformationGPRS	<b>FCI GPRS</b>	Gprs Billing Package [56]	77	4D	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
initialDPGPRS	<b>IDP GPRS</b>	Gprs Scf Activation Package [51]	78	4E	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
releaseGPRS	<b>REL GPRS</b>	Gprs Release Package [53]	79	4F	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
eventReportGPRS	<b>ERG</b>	Gprs Event Handling Package [54]	80	50	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
requestReportGPRSEvent	<b>RRGE</b>		81	51	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
resetTimerGPRS	<b>RT GPRS</b>	Gprs Timer Package [55]	82	52	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
sendChargingInformationGPRS	<b>SCI GPRS</b>	Gprs Charge Advice Package [60]	83	53	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
<b>CAP Operations for SMS Control</b>							
initialDPSMS	<b>IDP SMS</b>	Sms Activation Package [61]	60	3C	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
furnishChargingInformationSMS	<b>FCI SMS</b>	Sms Billing Package [66]	61	3D	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
connectSMS	<b>CON SMS</b>	Sms Connect Package [62]	62	3E	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
requestReportSMSEvent	<b>RRB SMS</b>	Sms Event Handling Package [65]	63	3F	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
eventReportSMS	<b>ERB SMS</b>		64	40	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
continueSMS	<b>CUE SMS</b>	Sms Continue Package [63]	65	41	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
releaseSMS	<b>REL SMS</b>	Sms Release Package [64]	66	42	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)
resetTimerSMS	<b>RT SMS</b>	Sms Timer Package [67]	67	43	0 4 0 0 1 21 3 (4)	0 4 0 0 1 22 3 (4)	0 4 0 0 1 23 3 (4)

Table A - 20. CAP Operations for CAMEL Call, SMS and GPRS control.

### **A.3.5.2 CAMEL Call Control**

From CAMEL phase I call control is defined for mobile originated, mobile terminated or mobile forwarded calls.

#### **A.3.5.2.1 Detection Points (DP)**

DPs compose call process points under which service logic notifications may occur as well as transfer of call handling from a gsmSSF to a gsmSCF. Typically, they are associated to events related to ISUP message arrivals at a (G)MSC during the process of a call.

A DP can be “armed” in order to notify the gsmSCF that the DP came upon, and potentially allowing the gsmSCF to influence subsequent handling of the call. If the DP is not armed, the processing entity continues the processing without gsmSCF involvement.

Three different types of DPs are identified for CAMEL call control:

- Trigger Detection Point - Request (TDP-R). This detection point is statically armed and initiates a CAMEL control relationship when encountered and there is no existing relationship due to the same CSI. Processing is suspended when the DP is encountered.
- Event Detection Point – Request (EDP-R). This detection point is dynamically armed within the context of a CAMEL control relationship. Processing is suspended when encountering the DP and the gsmSSF waits for instructions from the gsmSCF.
- Event Detection Point – Notification (EDP-N). This detection point is dynamically armed within the context of a CAMEL control relationship. Processing is not suspended when encountering the DP.



### A.3.5.2.2 Basic Call State Model (BCSM)

BCSM provides a high-level model for describing the required actions from the MSC/VLR or GMSC for the establishment, maintenance and eventual redirect of communication paths needed for the call participants. It identifies the basic call processing points every time operator specific service logic instances, accessed by a gsmSCF, are enabled of interacting with call control capabilities.

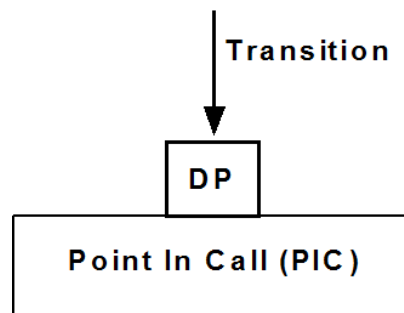


Figure A - 70. Basic components identified at the BCSM.

#### A.3.5.2.2.1 Originated BCSM (O-BCSM)

The O-BCSM is used to describe the actions in an MSC during originating (MSC), forwarded (MSC or GMSC) and trunk originating (MSC) calls.

When encountering a DP, the O BCSM processing is suspended at the DP and the MSC or GMSC indicates this to the gsmSSF which determines what action, if any, shall be taken if the DP is armed.

For gsmSCF initiated new calls the O-BCSM is initially suspended at DP Collected\_Info

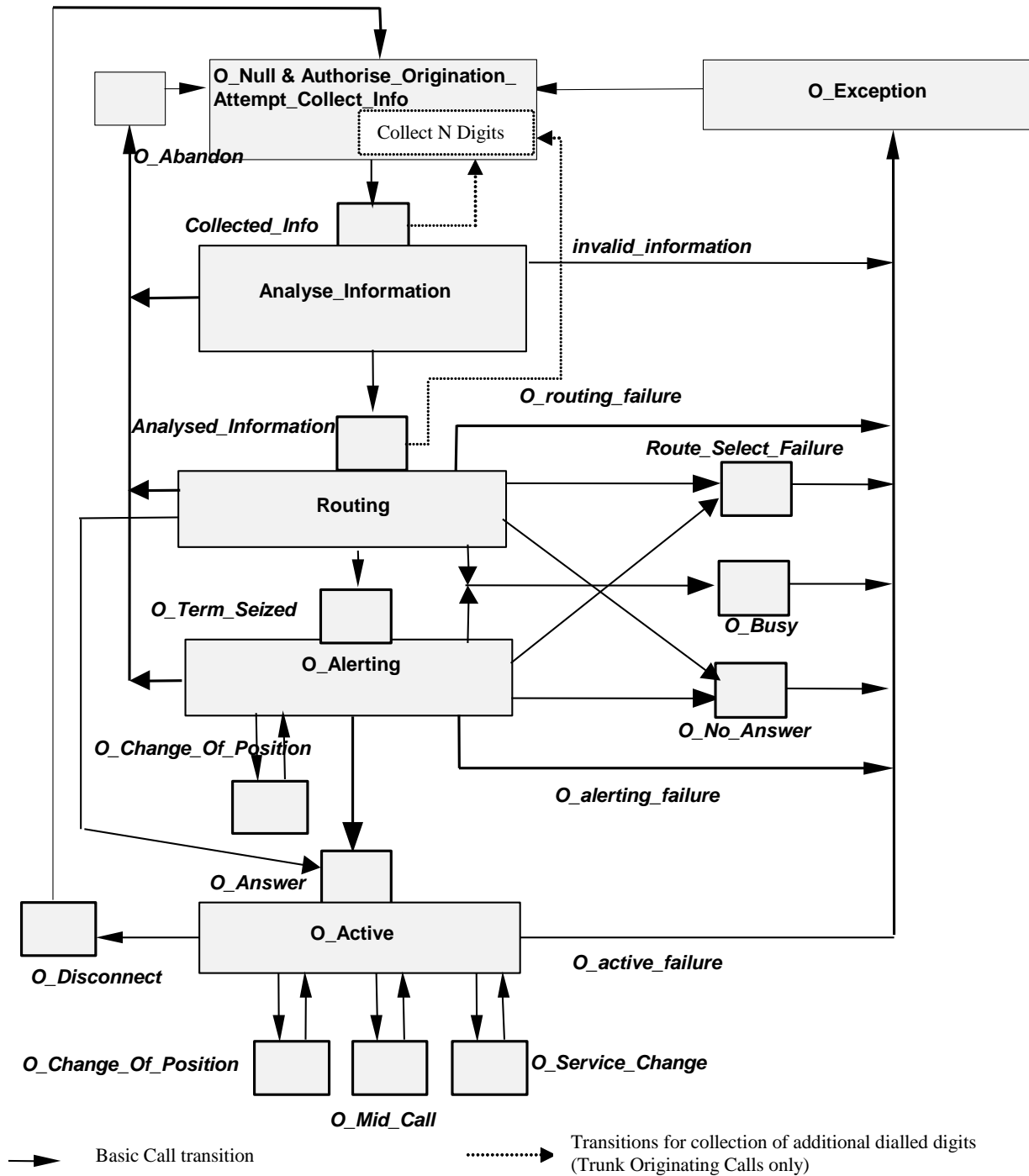


Figure A - 71. Originating BCSM for CAMEL [23].

The table below defines the different DPs which apply to mobile originating and forwarded calls and trunk originating calls.

Encountered DP	Implicit disarmed DPs											
	Collected_Info	Route_Select_Failure	O_Busy	O_No_Answer	O_Answer	O_Mid_Call Leg 1	O_Disconnect Leg 1	O_Disconnect any other Leg	O_Abandon	O_Term_Seized	O_Change_Of_Position	O_Service_Change
Collected_Info	X											
Route_Select_Failure		X	X	X	X			X		X		
O_Busy		X	X	X	X			X		X		
O_No_Answer		X	X	X	X			X		X		
O_Answer		X	X	X	X				X	X		
O_Mid_Call Leg 1 (note 1)						X						
O_Disconnect Leg 1						X	X		X		X	X
O_Disconnect any other Leg		X	X	X	X			X		X		
O_Abandon	X					X	X		X		X	X
O_Term_Seized										X		
O_Change_Of_Position (note 1)											X	
O_Service_Change (note 1)												X

Note 1: if the Automatic Rearm IE was present in the Request Report CSM Event information flow for the O\_Change\_Of\_Position DP, O\_Service\_Change or the O\_Mid\_Call DP and armed as EDP-N, then the DP shall be automatically rearmed by the gsmSSF when it is encountered.

Table A - 21. Implicit disarmed DPs in the O-BCSM.

Next figure displays a call flow diagram example as for the O-BCSM. Only CAP messages are shown between the gsmSSF at the MSC and the gsmSCF at the SCP. In this example, after reception of CAP ACR O\_Disconnect Leg 1 DP is encountered as the calling part runs out of credit, then CAP REL message is sent to release the call and therefore, the established CAMEL relationship.

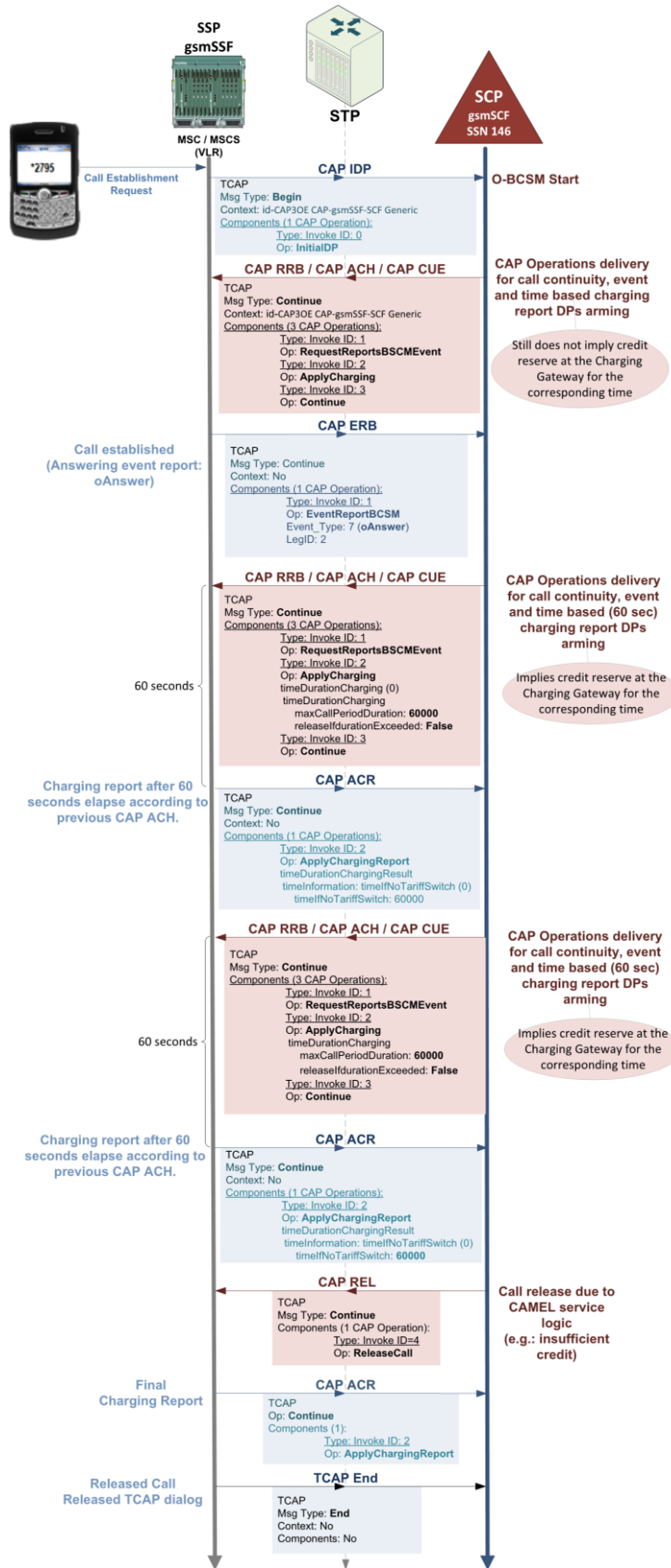


Figure A - 72. CAMEL O-BCSM call flow example (Calling party runs out of credit).

**A.3.5.2.2 Terminated BCSM (T-BCSM)**

The T-BCSM is used to describe the actions in a GMSC and in a VMSC during terminating calls. When encountering a DP, the T BCSM processing is suspended at the DP and the GMSC or VMSC indicates this to the gsmSSF which determines what action, if any, shall be taken if the DP is armed.

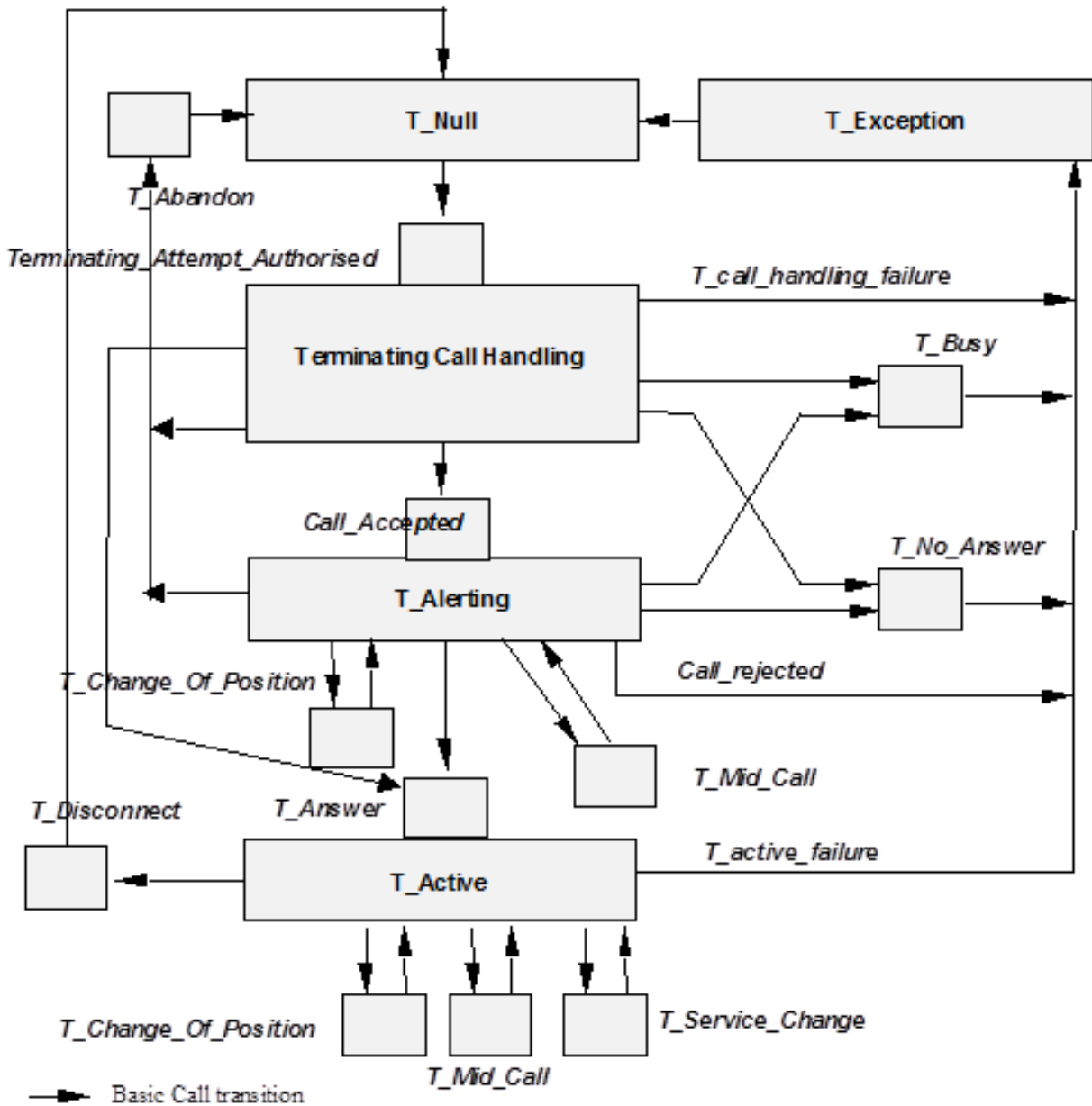


Figure A - 73. Originating BCSM for CAMEL [23].

Encountered DP	Implicit disarmed DPs									
	T_Busy	T_No_Answer	T_Answer	T_Mid_Call Leg 2	T_Disconnect Leg 1	T_Disconnect Leg 2	T_Abandon	Call_Accepted	T_Change_Of_Position	T_Service_Change
T_Busy	X	X	X	X		X		X	X	X
T_No_Answer	X	X	X	X		X		X	X	X
T_Answer	X	X	X				X	X		
T_Mid_Call Leg 2 (note 1)				X						
T_Disconnect Leg 1					X		X			
T_Disconnect Leg 2	X	X	X	X		X		X	X	X
T_Abandon					X		X			
Call_Accepted								X		
T_Change_Of_Position (note 1)									X	
T_Service_Change (note 1)										X

Note 1: If the Automatic Rearm IE was present in the Request Report BCSM Event information flow for the T\_Change\_Of\_Position DP, T\_Service\_Change or the T\_Mid\_Call DP and armed as EDP-N, then the DP shall be automatically rearmed by the gsmSSF when it is encountered.

Table A - 22. Implicit disarmed DPs in the T-BCSM.

Next figure displays a call flow diagram example including CAMEL specific messages as for the T-BCSM. In this example, after reception of CAP ERB T\_Disconnect Leg 1 DP is encountered (the calling party released the call), then the gsmSCF sends CAP FCI and CUE messages embedded in one TCAP message (two components) for finishing the established CAMEL relationship and provide charging information to the gsmSSF.

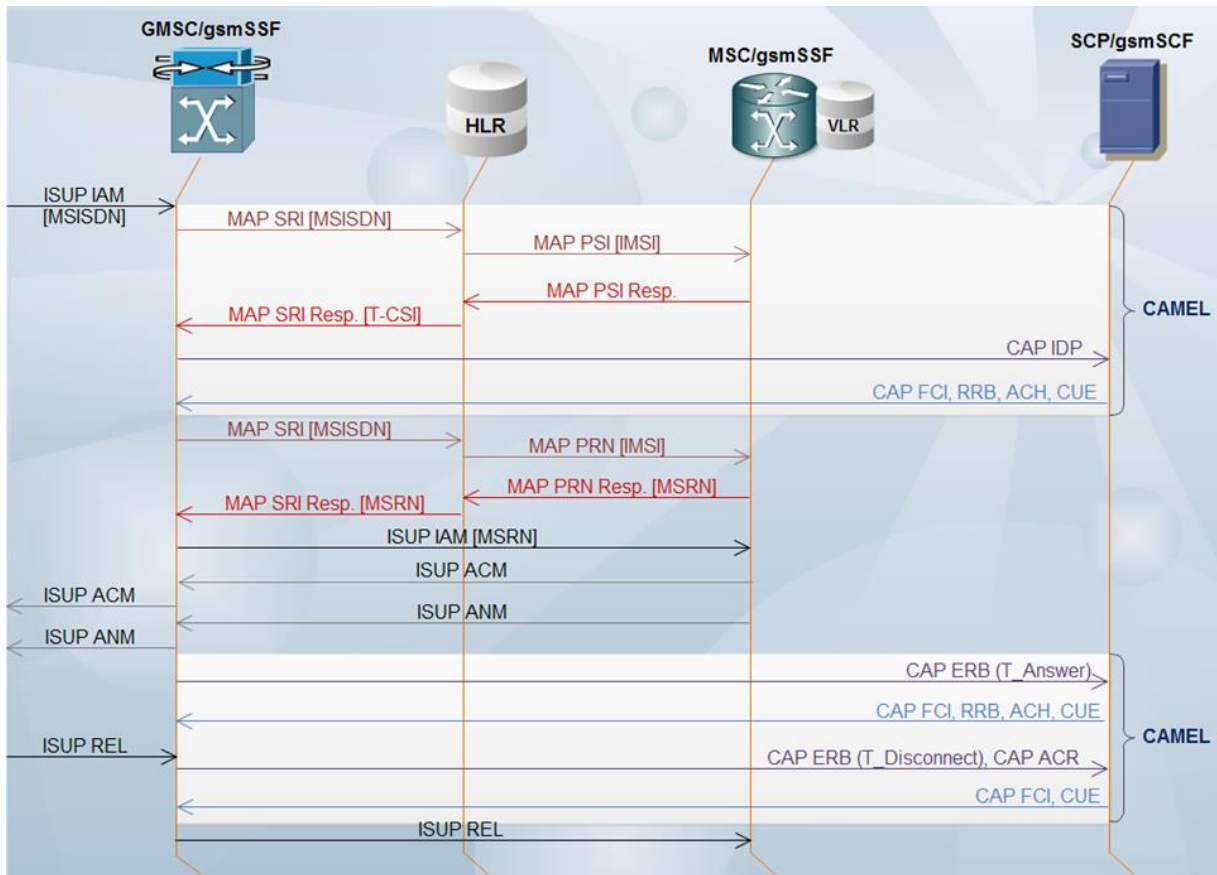


Figure A - 74 CAMEL T-BCSM example (calling party disconnects).

### A.3.5.3 CAMEL GPRS Control

CAMEL (phase III) introduces control for either GPRS session or PDP context (PDPc). CAMEL phase III constitutes the least one regarding CAMEL Subscription Information (CSI) to be supported by the user in order to accessing the services offered by the GPRS Packet-Switched Network.

CAMEL GPRS control occurs strictly through a CAMEL dialog between the SGSN and an SCP. The SGSN contains the gprsSSF (analogue to gsmSSF within a MSC or GMSC), which establishes a bond with the gsmSCF at the SCP. The control protocol between both functions is CAP v3, which differs substantially in its conception from the BCSM.

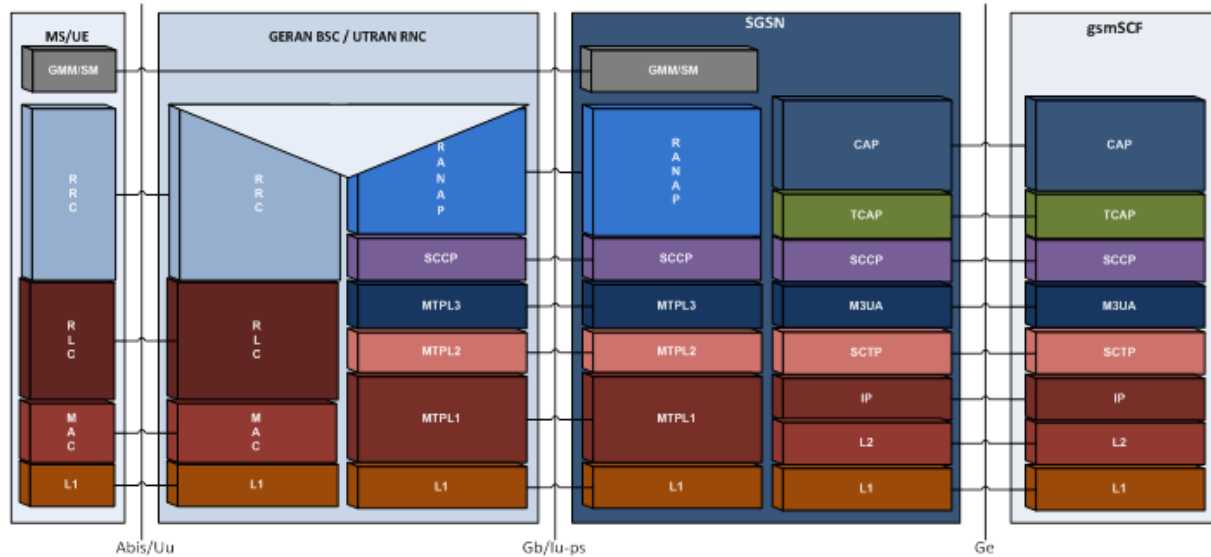


Figure A - 75. GPRS CAMEL control stack diagram.

The SGSN retrieves the user's GPRS-CSI from the HLR, which is bounded to the SGSN in the "GPRS/IMSI Attach" procedure. From "GPRS/IMSI Attach" procedure success either GPRS sessions or PDP contexts (Packet Data Protocol contexts) may be established via the GGSN with other Packet Data Networks –PDNs– (e.g.: Internet).

As every CSI, GPRS-CSI consists of one or more TDPs (Trigger Detection Points). Next table exhibits GPRS-CSI information elements as well as GPRS TDP definitions most probably included in it.

<b>GPRS-CSI</b>	
Element	Description
TDP List	Includes the list of TDPs. Each TDP in GPRS-CSI represents a TDP in one of the two GPRS state models, from where a CAMEL service can be invoked.
CAMEL capability handling	This element indicates the CAP version to be used in CAMEL dialogs. For GPRS CAMEL control, it will always be CAP v3.
<b>GPRS TDP List</b>	
Element	Description



TDP	Indicates the current position in the GPRS state model.
Service Key	Service key to use at the invocation of a CAMEL service.
gsmSCF	Address (in a Global Title format) of the SCP to which the CAMEL service invocation will be directed.
Default Handling	Handler indicator to be used by the gprsSSF in case of CAMEL dialog failure; one of two options will be taken: Continue or Release.

Table A - 23. Information Elements for GPRS Control.

#### A.3.5.3.1 GPRS Attach

A Mobile Station (MS) or User Equipment (UE) must achieve a registration procedure known as “GPRS Attach” in order to access to GPRS services. Through this procedure, the MS or UE must provide its identity and an indicator of which type of registration shall be executed (A/Gb mode –for GERAN access- or lu mode –for UTRAN access-). The «GPRS Attach» is performed with the SGSN. During this procedure, the SGSN contacts the HLR so as to perform Routing Area Update & Location Area Update. During the location area update, the SGSN and HLR may execute CAMEL subscription capabilities negotiation procedures, similarly as how it's done during registration at an SSP (MSC or GMSC) for call control.

After successful GPRS registration, the MS/UE is in READY state or PMM-Connected state (for A/Gb or lu mode), meanwhile MM (Mobility Management) contexts between MS/UE and SGSN become established. PDP contexts may be established beyond this point in time.

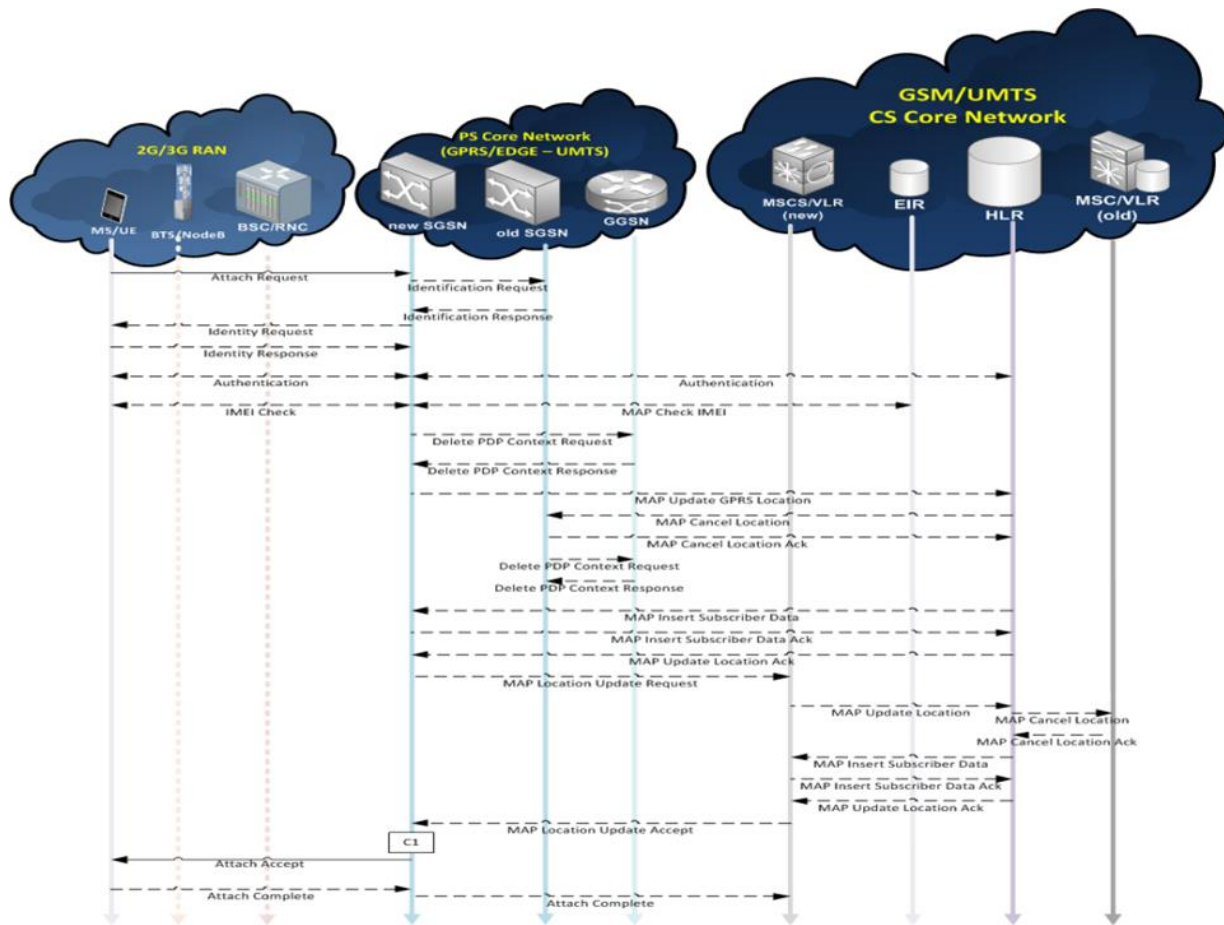


Figure A - 76. GPRS Attach procedure.

### A.3.5.3.2 GPRS Attach/Detach State Model

GPRS Attach/Detach State Model is used for behaviour modelling regarding GPRS attach/detach procedures. As soon as a DP is met, the processing is suspended at that DP in the meantime the SGSN indicates this event to the gprsSSF, which will determine what action to take (if it exists a determined one for that specific case) which shall be executed in case the DP is already armed.

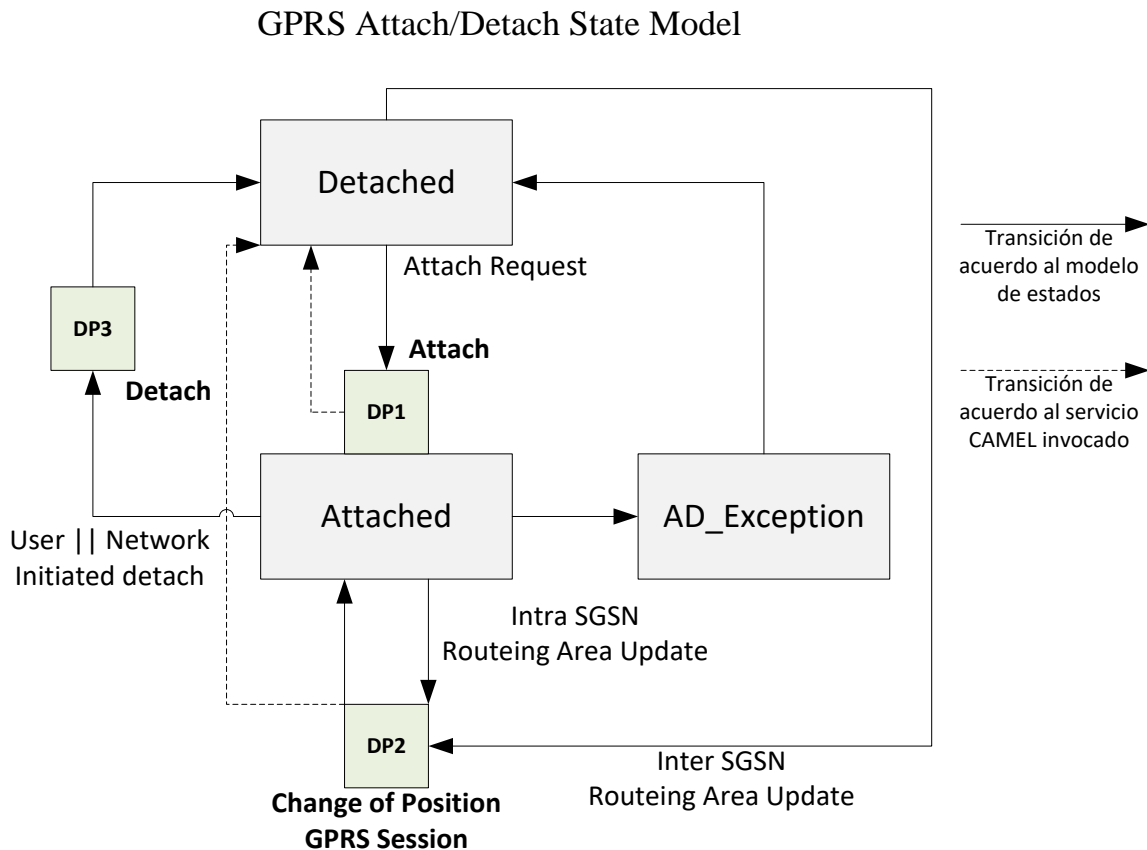


Figure A - 77. GPRS Attach/Detach State Model (3GPP TS 23.060).

**A.3.5.3.3 PDP Context (PDPc)**

The communication protocol at the Gn/Gp interface between GPRS nodes (SGSN/GGSN) is GTP (GPRS Tunneling Protocol), specified by 3GPP TS 29.060. From UMTS onwards (3G), GTP is also used between the SGSN and the RNC (Radio Network Controller). GTP purposes includes the following features:

- GPRS Control – Includes SGSN attach, PDPc creation and termination, RAU (Routing Area Update), etc. These are GTP-C (control) proficiencies.
- Payload Transfer – This GTP proficiency, part of GTP-U (user), s used for transmitting data payload through a tunnel, which consists of a logical data

connection established between SGSN and GGSN (for GERAN access) or between RNC and GGSN (for UTRAN access).

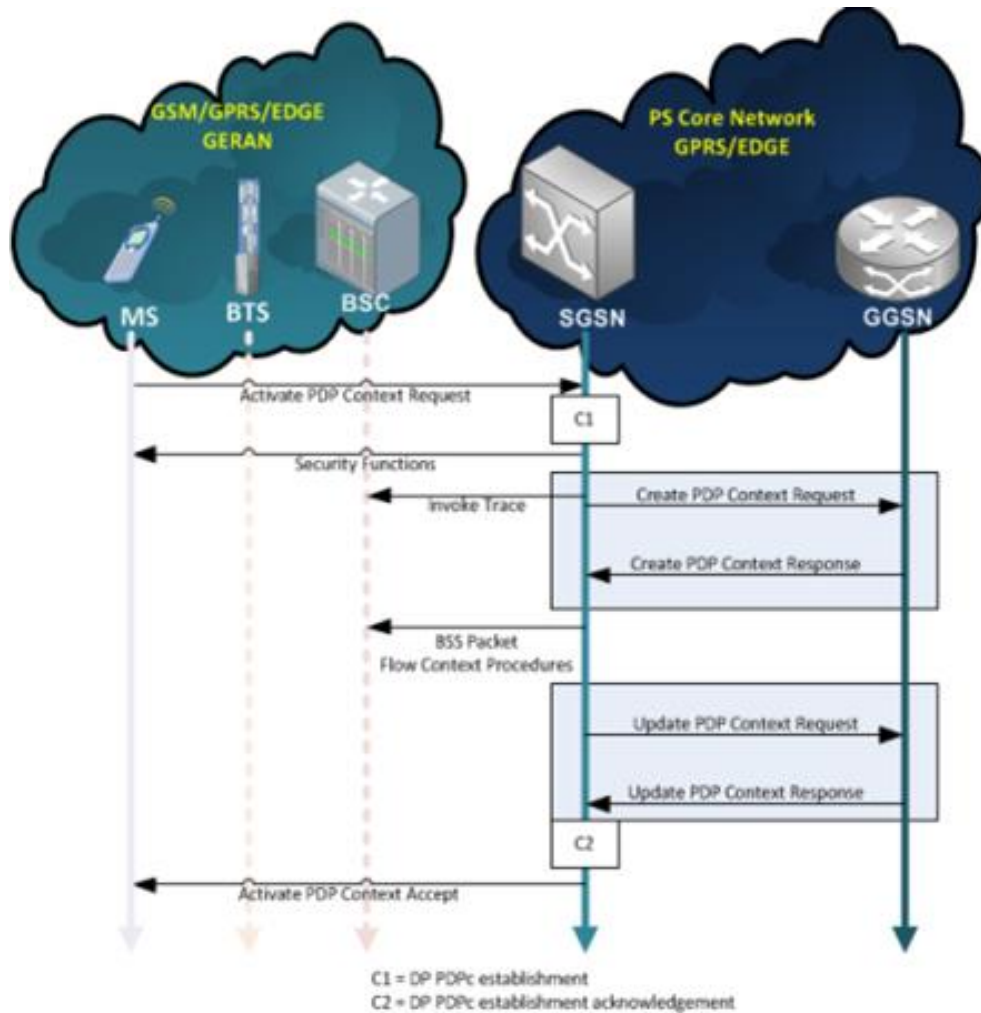


Figure A - 78. PDPc establishment for GERAN type of access.

The PDPc is then the data channel established between the user and the GGSN. GTP-U messages transmitted through a PDPc contain the T-PDU (Traffic Packet Data Unit), which consist in data units used for information transfer (payload). IP (or other protocol) packets embedded within a T-PDU, are transferred from the GGSN to the PDN. Multiple information elements such as QoS, APN, etc., are provided by whom initiates the PDPc. Both SGSN and GGSN nodes may also determine certain PDPc information elements.

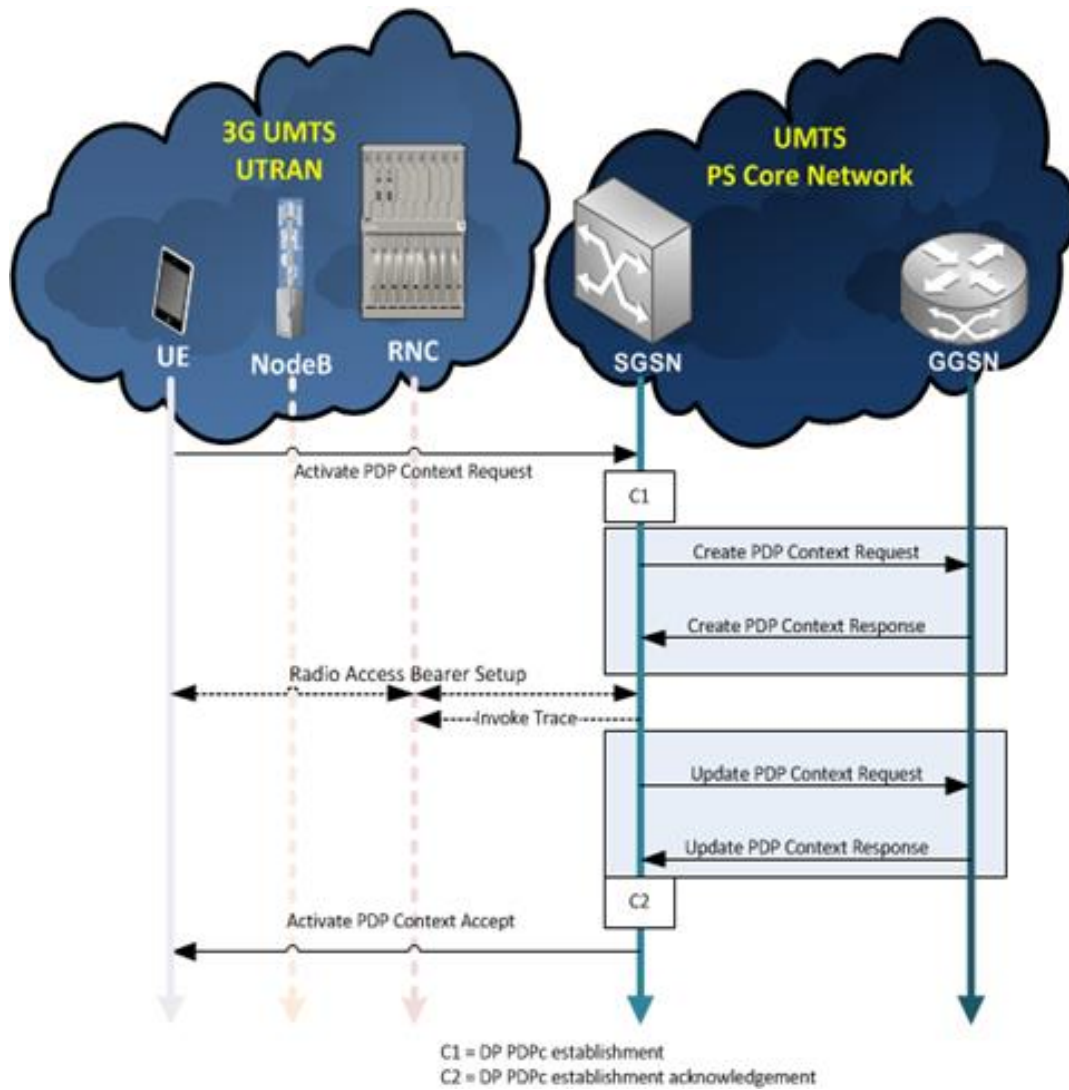


Figure A - 79. PDPc establishment for UTRAN type of access.

Element	Description
<b>End User Address</b>	Contains the address to use by the PDN to access the application at the MS/UE which has already established a PDPc. Usual addressing protocols: IPv4, IPv6, PPP, etc.

<b>Quality of Service Profile</b>	<p>Quality of Service (QoS) defines several parameters for PDPc, namely:</p> <ul style="list-style-type: none"> <li>• Uplink (UE -&gt; Network) maximum bit rate;</li> <li>• Downlink (Network -&gt; UE) maximum bit rate; <ul style="list-style-type: none"> <li>• Uplink granted bit rate;</li> <li>• Downlink granted bit rate;</li> <li>• Peak throughput.</li> </ul> </li> </ul>
<b>Access Point Name (APN)</b>	<p>The APN defines access to the PDN. Its maximum length is 100 octets and is composed of two sections: NI (Network Identifier) and OI (Operator Identifier):</p> <ul style="list-style-type: none"> <li>• NI (Network Identifier): with a topmost of 63 octets it's composed by one or more labels, containers of a realm name according to established rules by the Domain Name Server (DNS). Identifies the Internet domain point at which the data connection is established.</li> <li>• OI (Operator Identifier) –optional-. Consists of three labels including operator, group and country identifiers (e.g.: internet.tigo.gt, mnc002.mcc655.gprs, etc.)</li> </ul>
<b>Charging Id</b>	<p>Comprises a number assigned by the GGSN when a PCPc has been activated by the SGSN. The Charging Id is used together with the GGSN Address to uniquely identify a PDPc.</p>
<b>GGSN Address</b>	<p>Address that identifies the GGSN at which the PDPc has been established.</p>
<b>PDP initiation type</b>	<p>This parameter indicates if the PDPc has been established under user or network initiative.</p>

Table A - 24. PDPc Information Elements for GPRS Control.

#### A.3.5.3.3.1 GPRS PDP Context State Model

The GPRS PDP Context State Model is used for behaviour modelling regarding involved procedures for PDP context establishment. For each PDPc a GPRS PDP Context State Model exists. As soon as a DP is met, the processing is suspended at that DP in the meantime the SGSN indicates this event to the gprsSSF, which will determine what action to take (if it exists a determined one for that specific case) which shall be executed in case the DP is already armed.

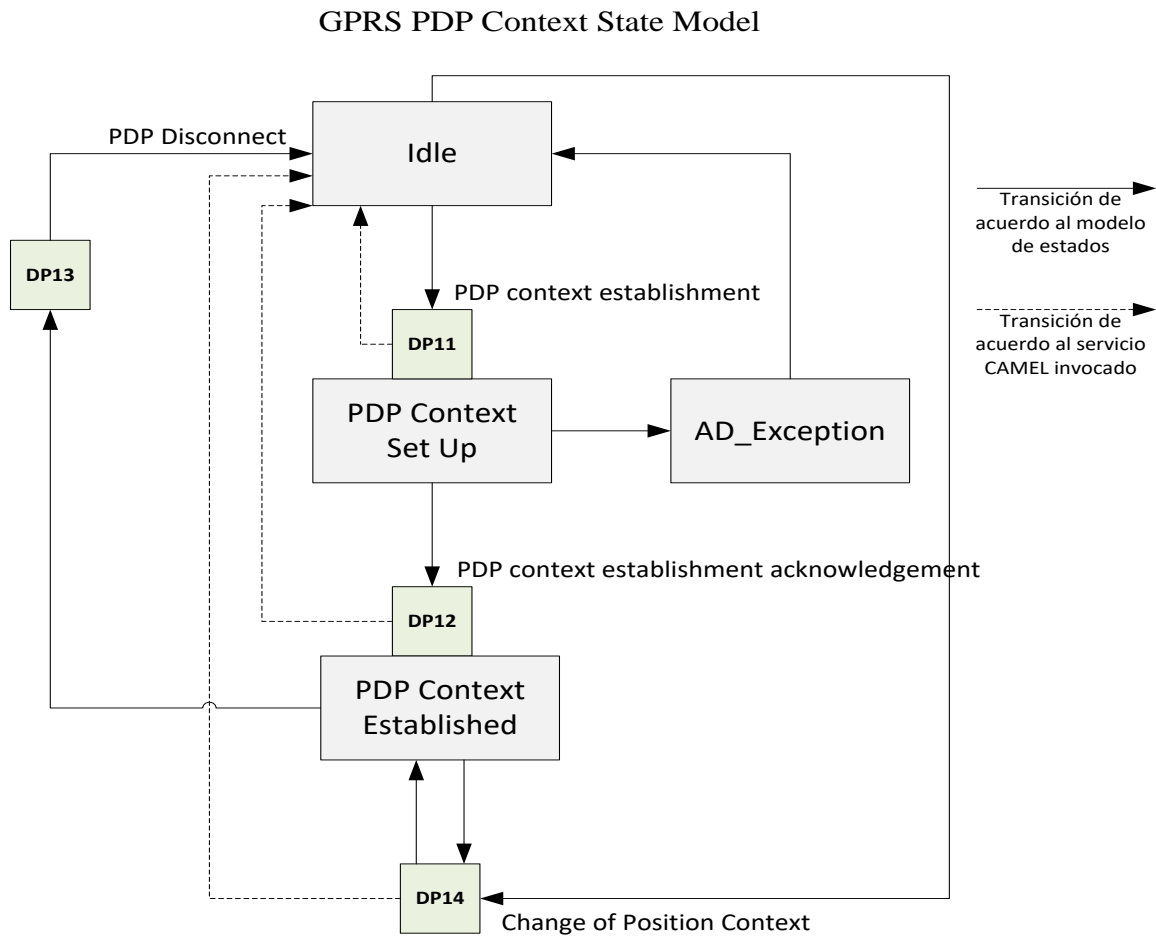


Figure A - 80. GPRS PDP Context State Model.

#### A.3.5.3.4 GTP Tunnel

A GTP tunnel is needed for transmitting packets between an access network user and an external packet data network. Each GTP tunnel whereby GTP-U messages can be transmitted is associated with a path controlled by GTP-C. A GTP logic control path may control one or several tunnels.

At the user plane (GTP-U), the GTP tunnel is defined for each PDPc or MBMS (Multimedia Broadcast/Multicast Service) and/or each RAB (Radio Access Bearer) belonging to the RNC. At the control plane (GTP-C), the GTP tunnel is defined for every PDPc with the same PDN connection (for tunnel management or UE specific

MBMS messages), for each MBMS service (for specific MBMS messages) or for each UE (for other type of messages). A GTP tunnel is identified in each node with a TEID (Tunnel Endpoint Identifier), an IP address and an UDP port.

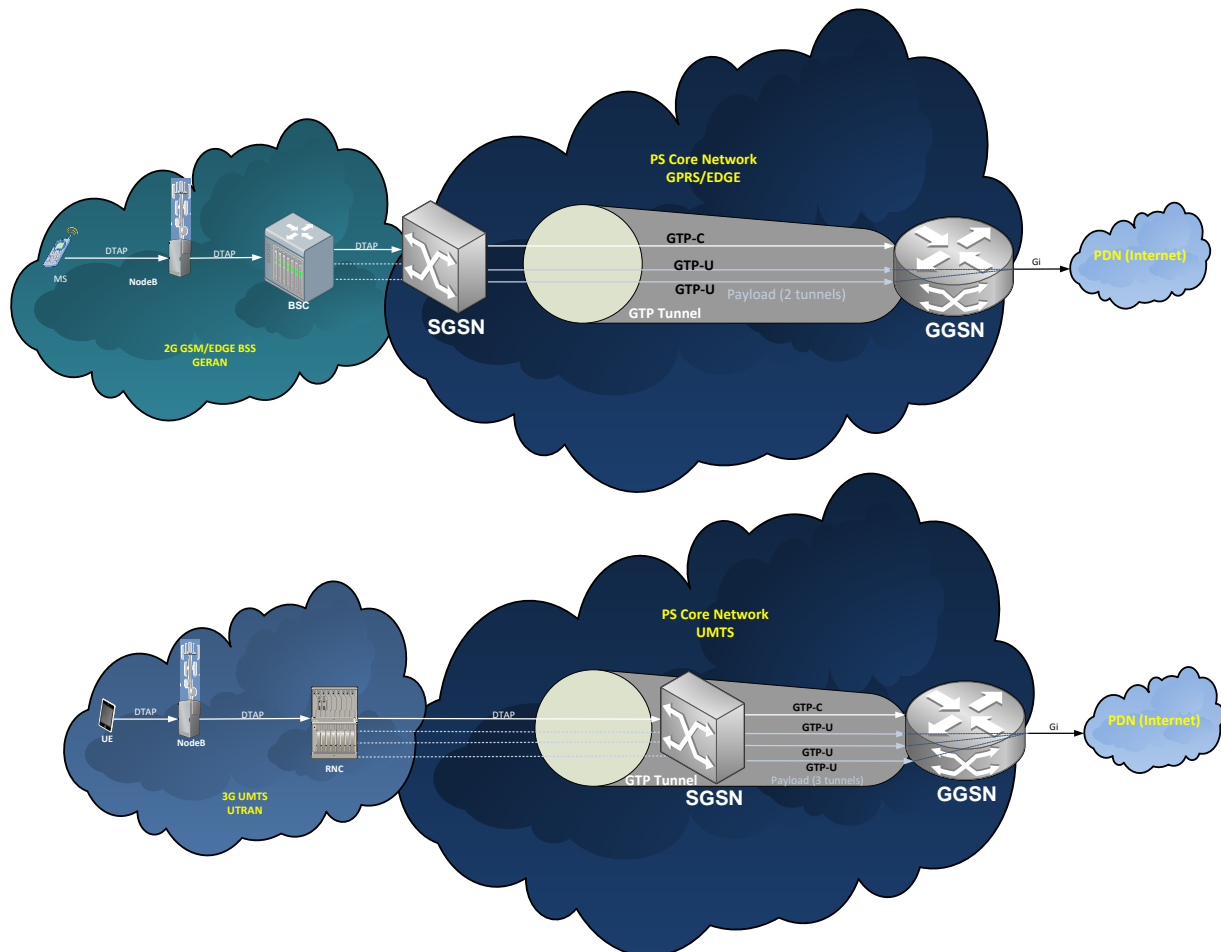


Figure A - 81. GTP tunnel examples for GERAN or UTRAN type of access.

### A.3.5.3.5 GPRS Control Scenarios

#### A.3.5.3.5.1 Scenario 1 in GPRS Control

So called «Scenario 1» allows GPRS session CAMEL control & multiple PDP contexts within a single GPRS dialog. In other words, a unique CAMEL service is invoked for GPRS Attach/Detach State Model control, as well as individual GPRS



PDP Context State Models –independently treated from each other- related to the GPRS session in question.

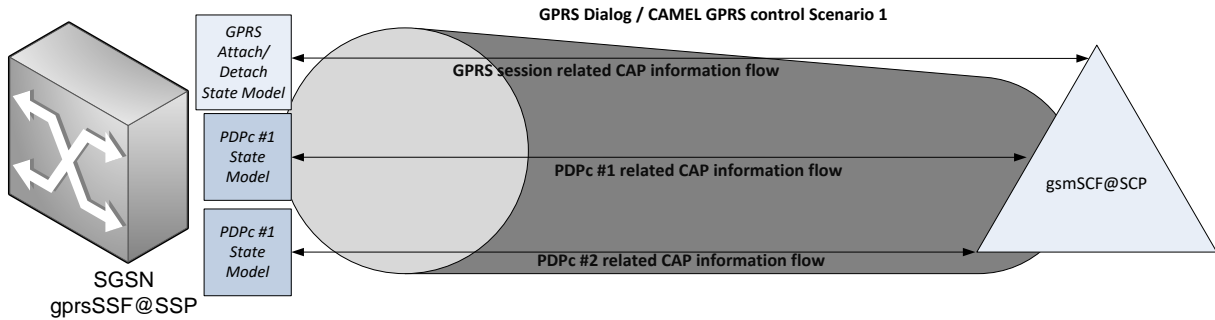


Figure A - 82. GPRS Control: Scenario 1 example.

**A.3.5.3.5.2 Scenario 2 in GPRS Control**

«Scenario 2» allows invoking a CAMEL service for each PDPc established by the subscriber. In other words, if for instance 7 PDPc are established for one GPRS session, then 7 CAMEL services are invoked (as well as their correspondent GPRS dialogs) and at least one GPRS PDP Context State Model for each PDPc at the SGSN.

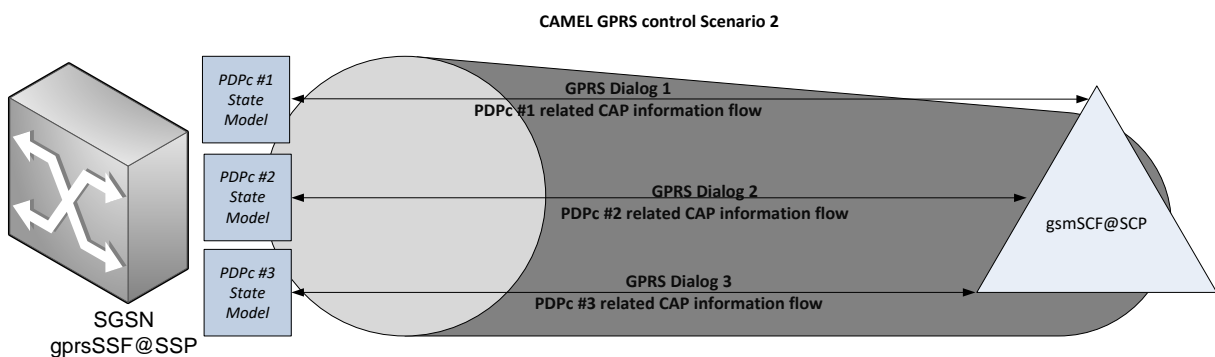


Figure A - 83. GPRS Control: Scenario 2 example.

### A.3.5.3.5.2.1 Sequence control for GPRS Control scenarios

CAMEL GPRS control scenarios 1 and 2 are excluding of each other, however, it is possible to invoke both of them in sequence as depicted in the following call flow diagram.

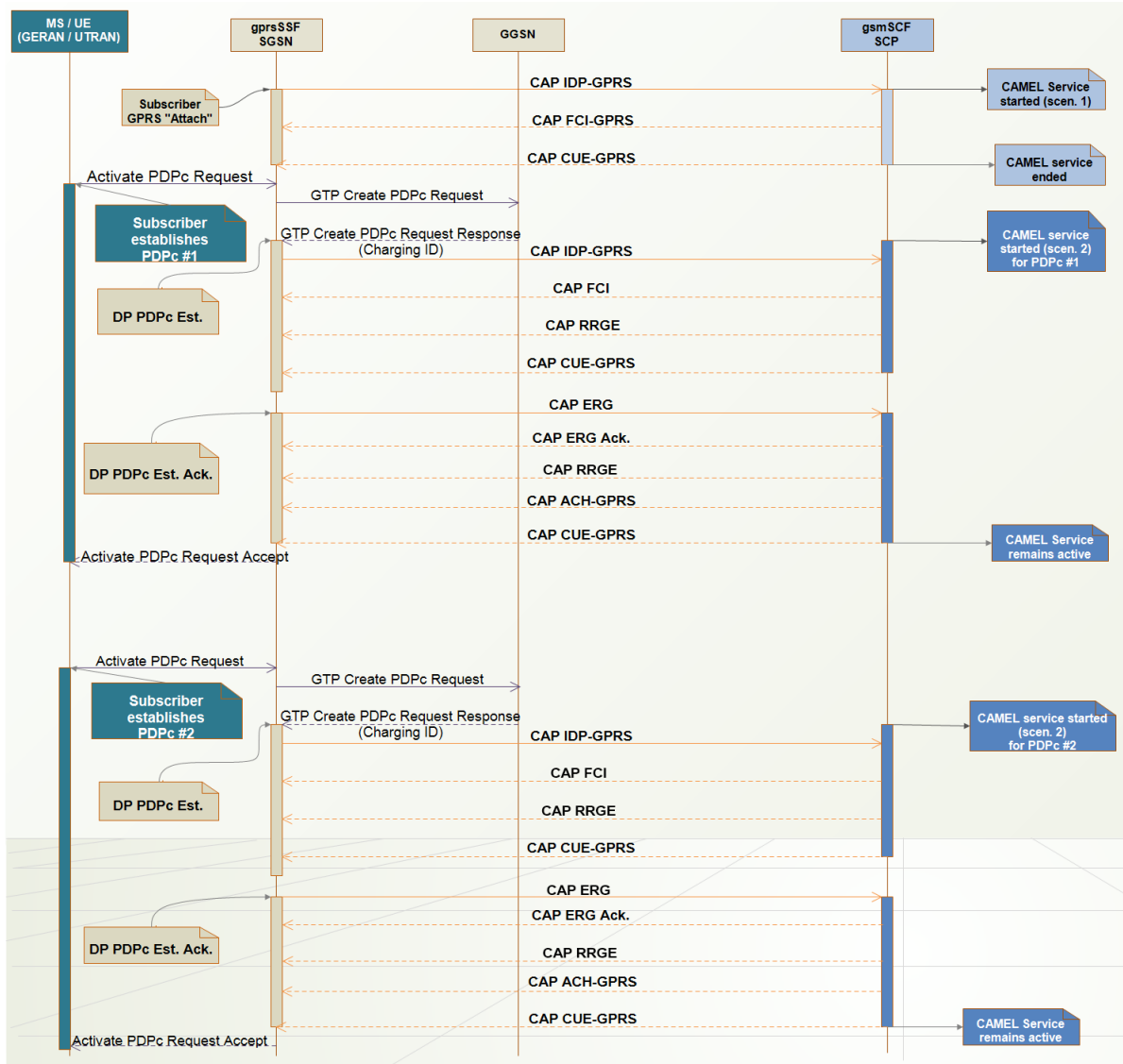


Figure A - 84. Example of sequential invocation of GPRS CAMEL Control Scenarios 1 and 2.

Next state diagram portrays the rules for reporting of events related to PDP contexts according to GPRS Control scenarios 1 and 2.

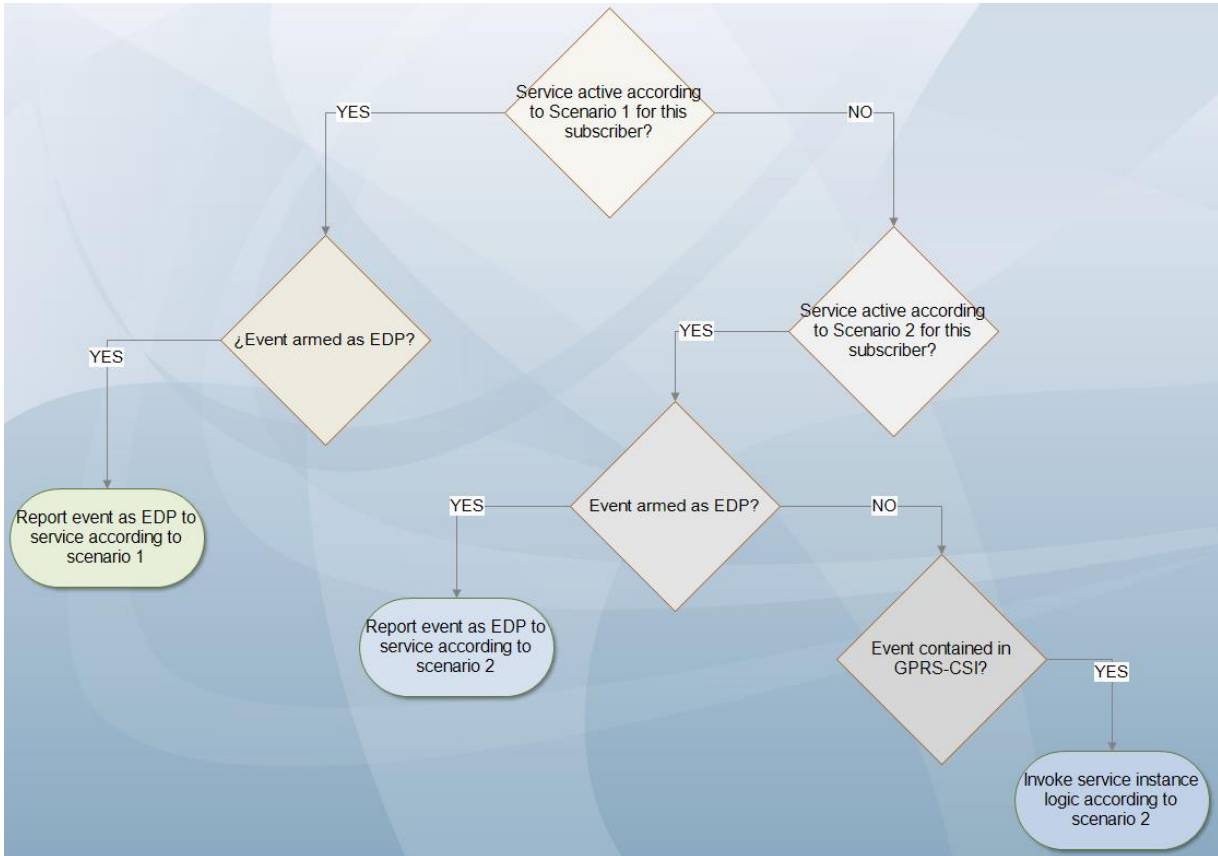


Figure A - 85. Rules for reporting of events related to PDP contexts according to GPRS control scenarios 1 and 2.

### A.3.5.3.6 GPRS Finite State Machine

The gprsSSF instantiates a FSM (Finite State Machine) whenever a CAMEL service is invoked. Its state is determined by the events occurring at the SGSN in the control plane between the gsmSCF and the gprsSSF. The state at the gprsSSF indicate the type of control the gsmSCF may invoke in the state models under control of the gprsSSF, as reflected in following diagrams for both scenarios. While in the first example, a gprsSSF FSM is controlling multiple state models: a GPRS session state model and several PDPc state models, in the second example each gprsSSF is controlling exactly one PDPc state model.

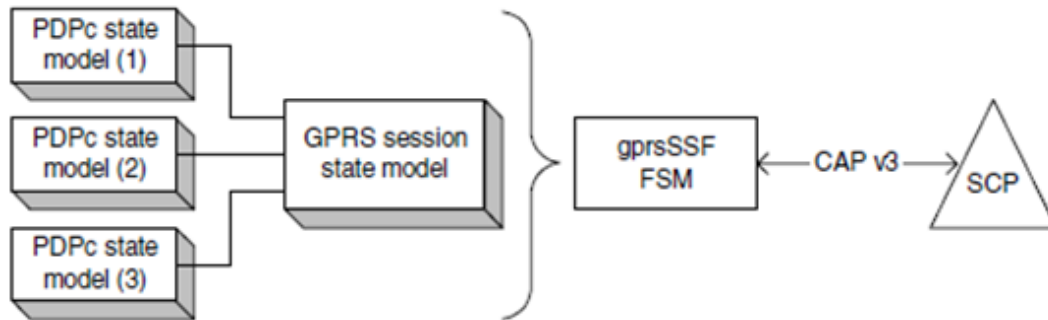


Figure A - 86. GPRS FSM service logic example as for scenario 1.

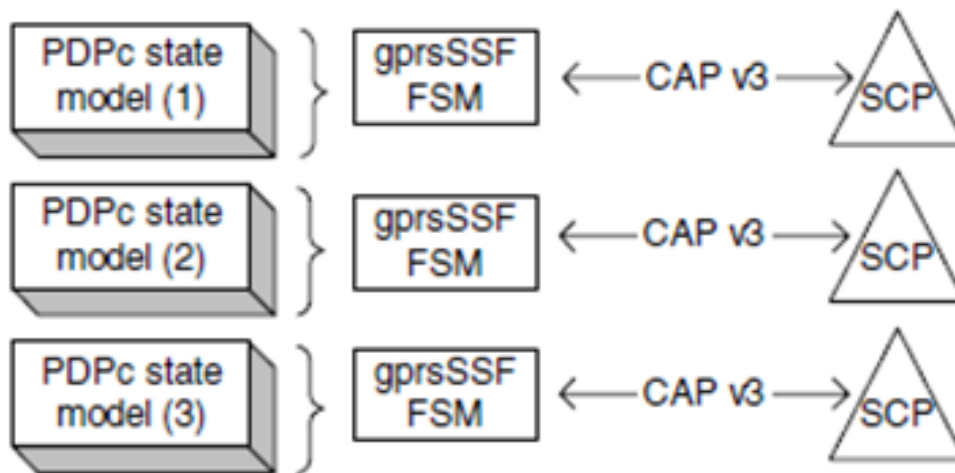


Figure A - 87. GPRS FSM service logic example as for scenario 2.

Following table lists and describes gprsSSF possible states. The diagram following the table represents how the gprsSSF FSM transits across the possible states.

gprsSSF FSM State	Description
Idle	<i>gprsSSF</i> is not currently invoked (idle state).
Wait_for_Request (WFR)	<i>gprsSSF</i> is invoked and waiting for service initial event (e.g. a <i>PDP context establishment</i> ).

Waiting_for_Instructions (WFI)	<i>gprsSSF</i> has established a CAMEL relationship with the <i>gsmSCF</i> and is waiting for instructions from the <i>gsmSCF</i> .
Monitoring (MON)	<i>gprsSSF</i> is currently active and monitoring a GPRS session or PDPc. A CAMEL relationship exists with the <i>gsmSCF</i> .

Table A - 25. *gprsSSF* FSM states description.

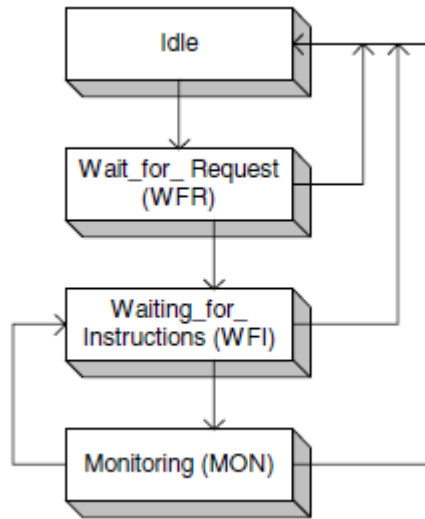


Figure A - 88. GPRS FSM transitions.

**A.3.5.3.7 Implicitly disarming rules for Detection Points in CAMEL GPRS Control**

Next tables display the rules for DP implicitly disarming rules. EDPs implicitly disarming rules are specified for either GPRS Attach/Detach State Model y GPRS PDP Context State Model, as an EDP is detected, irrespectively of its monitoring mode (Transparent, Notify and Continue, Request).

EDPs generically armed for GPRS PDP Context State Model should only apply at the end of a GPRS dialog. An explicit disarming is also possible. In the event of detecting either EDP armed in «Request» mode (EDP-R), every implicit EDP disarming shall take place previously to the EDP report and transition to WFI at the *gprsSSF* (in case of not being yet suspended at WFI state).

In both tables, the «X» means that if a DP occurs, independently of gsmSCF arming and reporting), it's implicitly disarmed. It is possible to rearm an implicitly disarmed DP.

DP Detected	DP implicitly disarmed					
	Change of Position GPRS Session	Change of Position Context	Detach	PDP Context Establishment	PDP Context Establishment Acknowledgement	PDP Context Disconnection
Change of Position GPRS Session						
Change of Position Context						
Detach	X	X	X	X	X	X
PDP Context Establishment						
PDP Context Establishment Acknowledgement					X	
PDP Context Disconnection		X			X	X

Table A - 26. Implicitly disarmed DP rules for GPRS CAMEL scenario 2.

DP Detected	DP implicitly disarmed		
	Change of Position Context	PDP Context Establishment Acknowledgement	PDP Context Disconnection
PDP Context Establishment Acknowledgement		X	
PDP Context Disconnection	X	X	X
Change of Position Context			

Table A - 27. Implicitly disarmed DP rules for GPRS CAMEL scenario 2.

### A.3.5.3.8 TCAP Segmentation

TCAP dialog segmentation is a particular aspect of GPRS CAMEL control, opposite of how it is handled in CAMEL Call control, where the CAMEL dialog remains active for the whole duration of the call.

A particularly distinctive aspect of a PDPc or GPRS session is that a subscriber can be attached to an SGSN for long period of time (days or weeks). The «permanent connectivity» concept is the reason why a PDPc (by which a subscriber might connect to the Internet, a corporate LAN or the IMS) may be active for a long time. Then, a CAMEL service may remain active for the whole PDPc activity period. Therefore, keeping active TCAP dialogs simultaneously between the SGSN and SCP for handling a high number of PDPc becomes extremely inconvenient and potentially catastrophic. Then, by CAMEL phase III, TCAP dialog segmentation is introduced (only used for CAMEL GPRS control). Next figure exhibits the TCAP dialog

segmentation mechanism, framed under the GPRS FSM transit and the events happening in parallel at the signaling level or associated TCAP dialogs.

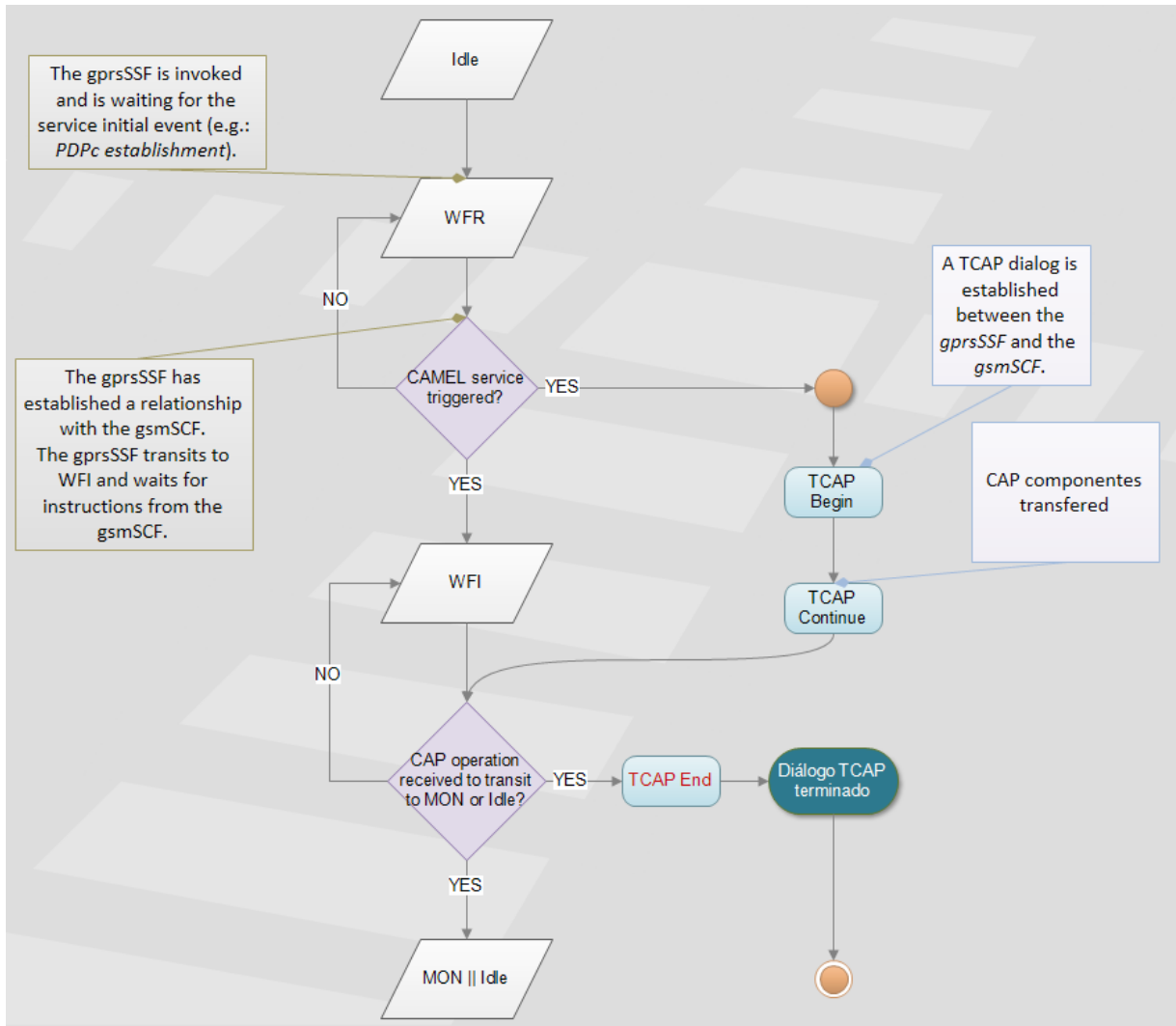


Figure A - 89. TCAP segmentation mechanism from the GPRS FSM perspective.

The following diagram depicts an example of CAMEL TCAP dialog segmentation under an established CAMEL relationship between the SGSN and an SCP (gprsSSF <-> gsmSCF).

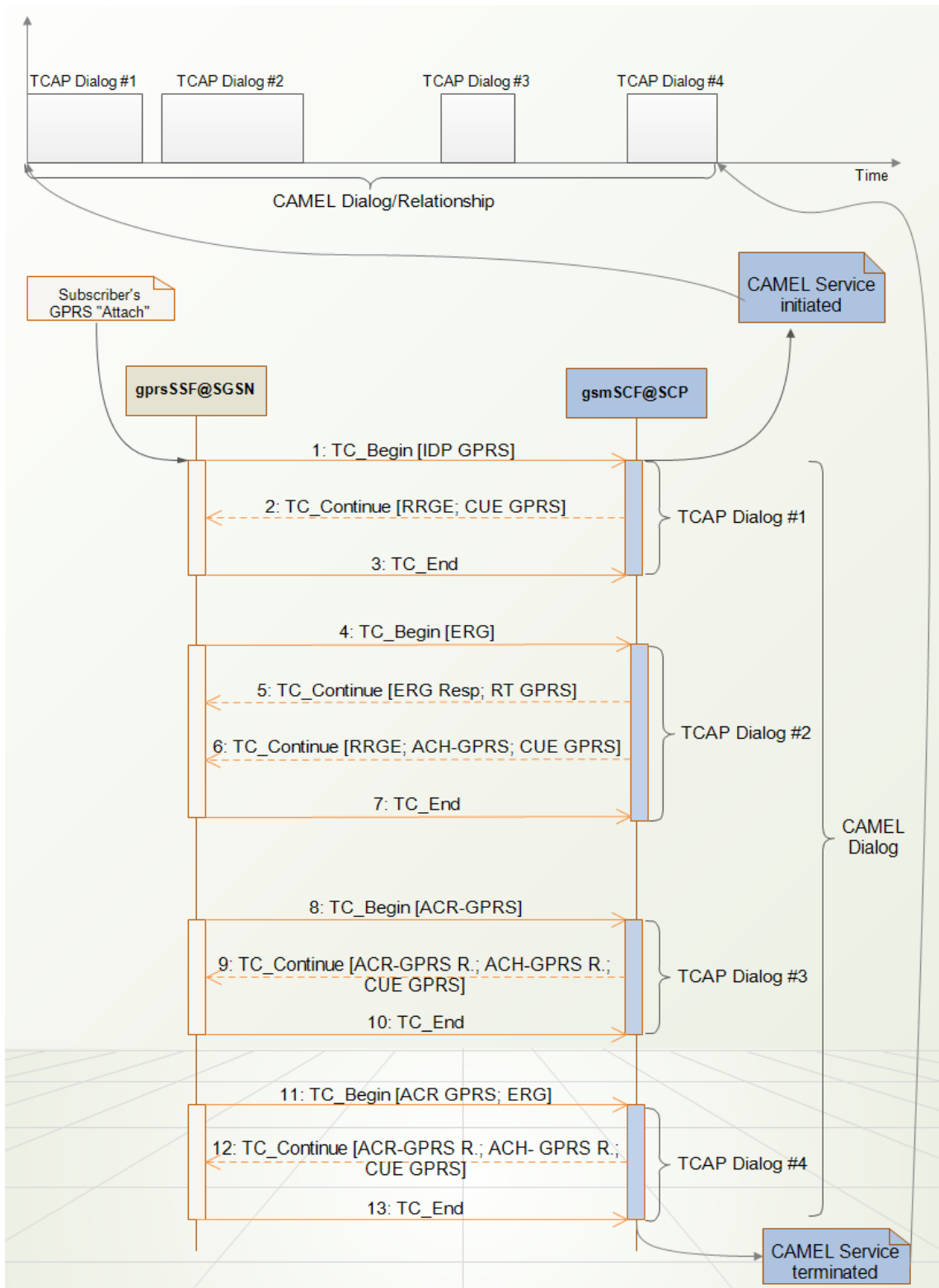


Figure A - 90. Example of TCAP dialog segmentation for CAMEL GPRS control.



### A.3.5.4 CAMEL SMS Control

Depending on subscription data, a subscriber may send SMS either via MSC, or SGSN. The MSC or SGSN use MAP signaling to transfer the SMS to the SMSC. After SMS arrival at the SMSC and is accepted, the SMS submission is considered successful. Delivery of the SMS to the destination is not part of the MO SMS functionality.

The SMS-IWMSC works as an interface between the 3GPP CS CN domain and the IT domain. The MSC and SGSN are part of the 3GPP CS CN domain, whereas the SMSC is part of the IT domain. The interface between MSC or SGSN and SMS-IWMSC is MAP as for [22]. The interface between SMS-IWMSC and SMSC is not defined in GSM/3GPP. Short Message Peer-to-Peer (SMPP); and Universal Computer Protocol (UCP) are mostly used for accessing the SMSC. The SMS-IWMSC is often integrated in the SMSC, then MAP signaling is used between the MSC and the combined SMSC and SMS-IWMSC node.

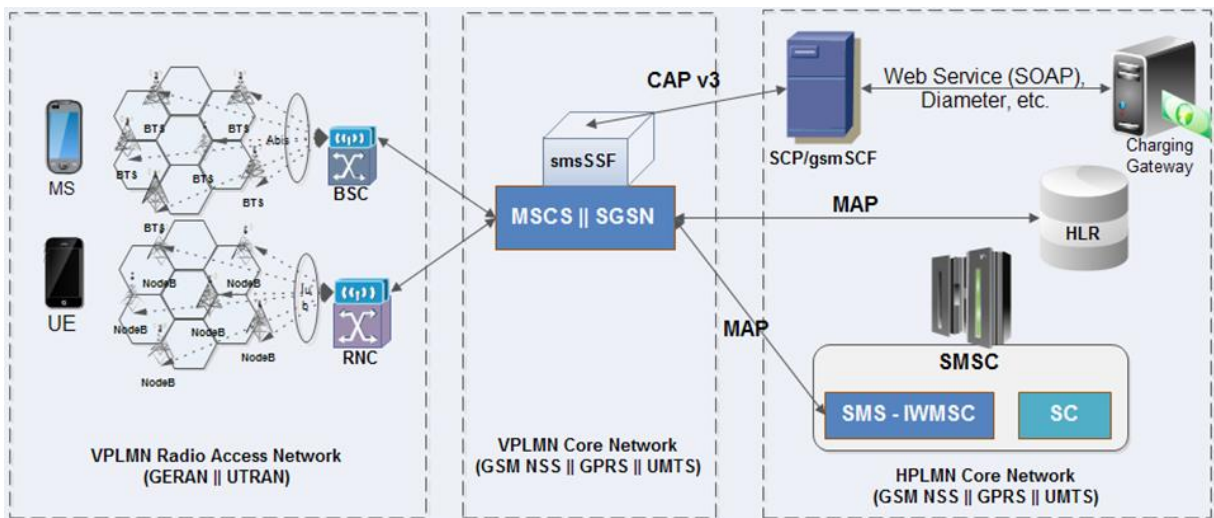


Figure A - 91. Network Architecture entities and interfaces for CAMEL SMS Control.

SMS CAMEL Control only applies to Mobile Originated SMS (MO-SMS), which is a subscribed service (MO-SMS-CSI to be sent from the HLR to the MSC or SGSN during the registration procedure). A CAMEL relationship must be established between the MSC or SGSN and the gsmSCF.

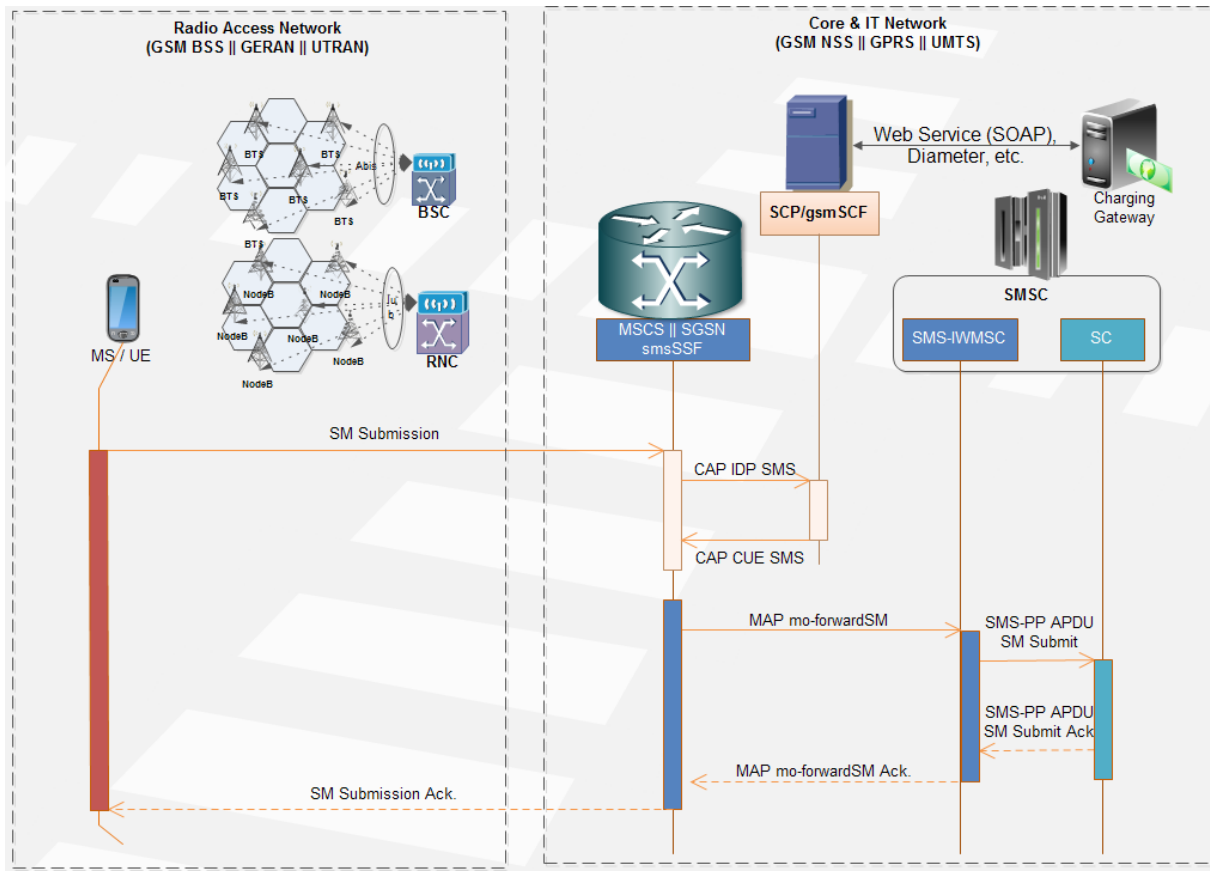


Figure A - 92. MO SMS CAMEL control signal flow.

### A.3.6 Introduction to Signaling Transport for SS7 over IP (SIGTRAN)

As part of Telecommunications convergence, the IETF defined a group of standards known as SIGTRAN (SIGnaling TRANsport). The objective was delivering a communication architecture of SS7 signaling messages over IP, or in other words, providing an interconnection between SS7 and IP networks without the need of tearing apart the existing network infrastructures/architectures.

Numerous benefits are provided by an IP network in comparison to an SS7 TDM based network, namely:

- More cost-effective infrastructure - TDM equipment is always more expensive than IP based ones.

- Transport efficiency - SIGTRAN removes E1s/T1s over SDH rings; IP communication over SDH or WDM guarantees a considerably superior throughput.
- Higher Bandwidth – SS7 networks' TDM based links capacity restrictions are eradicated.
- Enhanced flexibility and scalability – IP networks are much more flexible and easily scalable compared to SS7 networks.
- Easier implementation/compatibility - Signaling Gateways allow not altering the existent SS7 network, enabling future enhancements in a transparent mode.
- Improved services – Value Added Services (VAS) aggregation is much more accessible and easy to implement/deploy in IP networks compared to SS7 networks.

#### A.3.6.1 SIGTRAN Architecture Entities

To accomplish the task of exchanging information between SS7 and IP network entities, the following elements are integrated:

- **MGW** (Media Gateway) - A MGW handles calls/trunks, compresses and packetizes digitized speech and delivers data packets in both directions between PSTN/PLMN service switching points and the IP network. For ISDN type of calls from the PSTN, Q.931 signaling information is transported from the MGW to the MGC for its handling.
- **MGC** (Media Gateway Controller) - A MGC, typically known as "Softswitch", on one side handles resources registration and management of one or multiple MGW, and on the other side, exchanges ISUP messages with SS7 service switching points through a SGW.
- **SGW o SG** (Signaling Gateway) - A SGW or SG provides transparency in the signaling information exchange between a circuit-switched core network such as SS7 and an IP network. A SGW may terminate an SS7 signaling service or translating and dispatch SS7 packets to another SGW or an MGC. It then

achieves the major concern of IETF regarding SIGTRAN definition: interconnecting SS7 and IP networks transparently.

- **AS** (Application Server) – An AS comprises a logical entity serving a specific routing key (there is a one-to-one relationship between an AS and a routing key):

- ✓ **Routing Key** - A set of SS7 address/routing parameters, such as the MTP3 routing label (SIO, DPC, OPC, SLS) or MTP3-User specific fields (such as ISUP CIC, SCCP SSN), that uniquely defines the range of signaling traffic to be handled by a particular AS.

- ✓ **Routing Context** - A value that uniquely defines a routing key.

An example of an AS is a service switching point handling all call processing for a unique range of SS7 network trunks, identified by an SS7 routing label (SI, NI/MP, DPC, OPC, CIC range, SLS, etc.). Any database addressed through IP attending SCCP user's requests comprises an AS. Further examples of an AS are a SIP-AS, an IP HLR (HSS), an IP SCP (IM-SSF) or an MGC. An AS contains a group of one or more ASPs (Application Server Processes), one of which is actively processing traffic.

- **ASP** (Application Server Process) - An active or standby process instance of an AS. An ASP is defined by its SCTP Endpoint information (two IP addresses and a port). It can be configured to process signaling traffic for more than one AS.
- **IPSP** (IP Signaling Point) - An IPSP basically emulates an SS7 node that uses an IP network instead of traditional SS7 links. Multiple ASPs can be activated in an IPSP. An IPSP is essentially the same as an ASP, except that it uses an adaptation layer (e.g.: M3UA) in a point-to-point fashion. Conceptually, an IPSP does not use the services of a Signaling Gateway.
- **IF** (Interworking Function) – An IF constitutes a functionality for message exchange between protocols in an SG (e.g.: between MTP2/M2UA or SCCP/SUA). IF is not standardized; thus, manufacturers may implement it specifically according to their development environments.

### A.3.6.2 SIGTRAN protocol stack

The IETF defines in its Request for Comment 2719 (RFC 2719) an architecture for the SIGTRAN protocol stack, which basically consists of a three layers' model:

- **IP**: Internet Protocol
  
- **SCTP**: Stream Common Transport Protocol

An Adaptation Sublayer for specific support of service primitives required by a particular application signaling protocol. The IETF defines several sublayer adaptation protocols, namely: M2PA, M2UA, M3UA, SUA, IUA, V5UA, DUA. Only one at a time of this sublayer adaptation protocols can be implemented.

SCTP y M3UA will be described in this document. The rest of the aforementioned sublayer adaptation protocols are outside of the scope of this material (besides being the less used, are not yet implemented in Telestax' SS7 stack –Mobicents community or sponsored development dependent-).

#### A.3.6.2.1 Stream Control Transport Protocol (SCTP)

The IETF defines in its RFC 4960 the transport protocol of IP based applications for SIGTRAN, namely: **SCTP** (Stream Control Transport Protocol). TCP (RFC 793) is discarded for SIGTRAN due to the following limitations:

- Real-time applications delivery inefficiency – TCP's packet delivery sequential mechanism introduces delays and potential degradation of services demanding high bandwidth and immediate delivery.
- Sockets limitations – TCP's low sockets accessibility prevents high data transfer availability when multiple IP addresses remain vacant for the same entity, a capability named "multi-homing".
- Security - TCP is relatively vulnerable to denial of service attacks.

SCTP then remains as the transport protocol of signaling messages over IP networks. As TCP, it is connection-oriented, and besides solving the aforementioned TCP limitations, it occupies the following characteristics:

- Recognized data transfer, unduplicated, error free (through Adler 32 algorithm).
- Segmentation of data at application level.
- Adaptable transfer rate according to traffic conditions.
- Sequential data delivery via multiple frame flows or "multi-streaming" (with an optional ordered arrival of individual messages). SCTP uses streams as a means of decreasing the impact of head-of-line blocking. In SCTP, a stream is a unidirectional channel within an association. Streams provide the ability to send separate sequences of ordered messages that are independent of one another.
- High fault tolerance due to "multihoming". In other words, the multiple host assignment to each network entity allows high routing redundancy between ends.
- Optional user-datagram multiplexing within a unique SCTP packet (subject to MTU size restriction).

#### **A.3.6.2.1.1 SCTP Association**

Each end of an SCTP connection is named «SCTP endpoint», defined by the SCTP transport address, consisting of a group of IP addresses and an SCTP port. Both endpoints exchange information during the initialization process so as to establish what is termed as an SCTP association.

The next diagram exhibits an example of an SCTP association between two endpoints involving IP ASPs, distinguished as Host A and Host B. This example SCTP association del is given by the combination of both endpoints, i.e., Host A Endpoint [10.1.1.1/10.1.4.100:2905] and Host B Endpoint [10.1.1.10/10.1.4.120:2905].

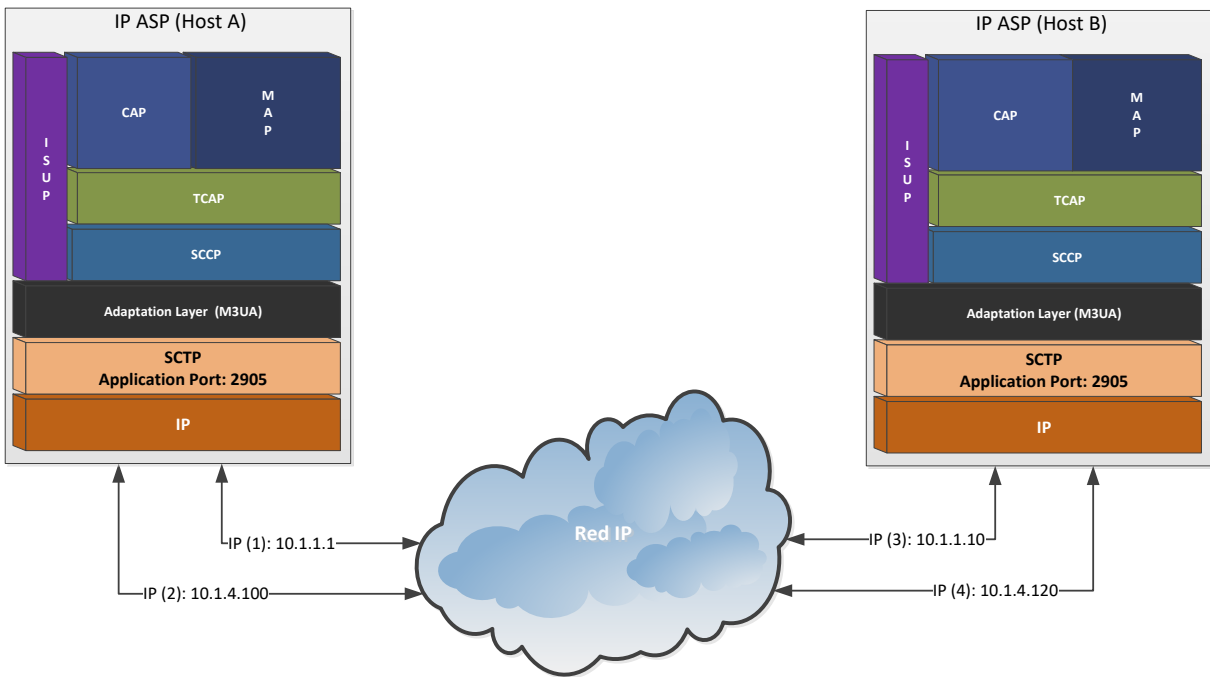


Figure A - 93. Sctp Association example for IP ASPs.

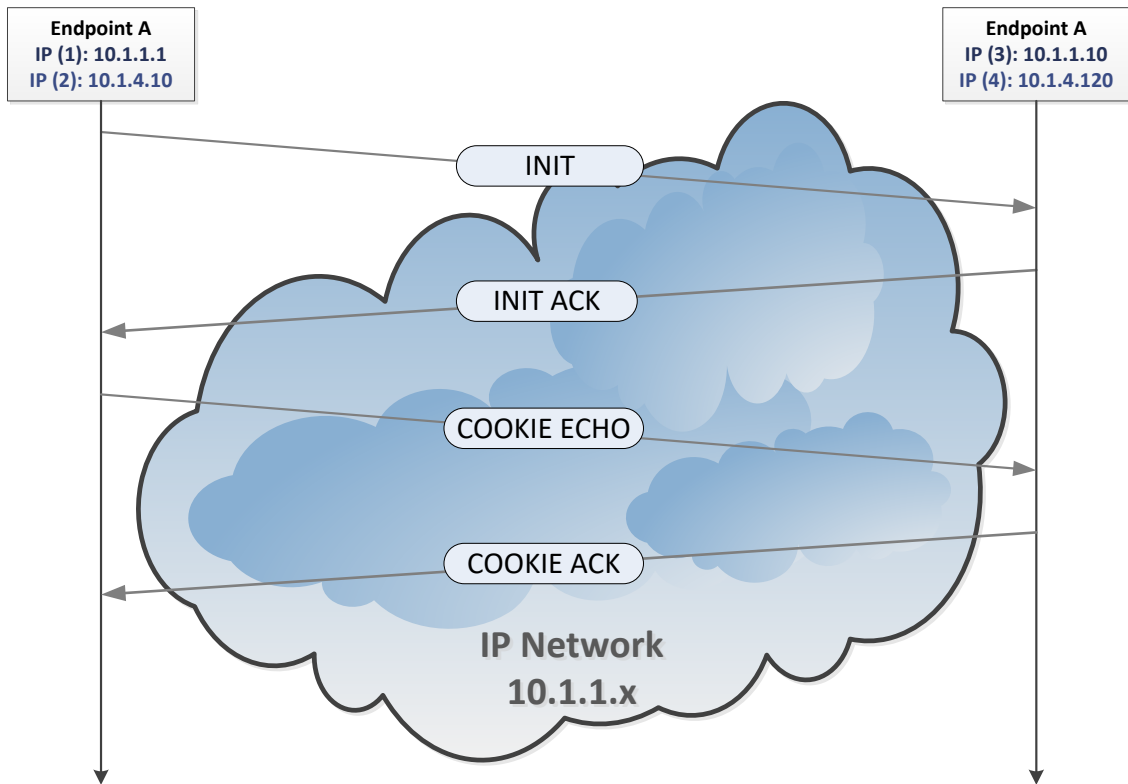


Figure A - 94. Sctp handshake example.

Connection-oriented as SCTP is, it follows a procedure to setup a communication relationship or association known as «handshake», like shown in the preceding signal diagram example.

### A.3.6.2.1.2 Multi-homing

The term known as “multihoming” provides redundancy to each end of an SCTP association. SCTP multihoming supports only communication between two end points, of which one or both are assigned with multiple IP addresses on possibly multiple network interfaces. Each address finds a different packet transceiving path through the IP network. The multihoming concept is graphically displayed in the following figure.

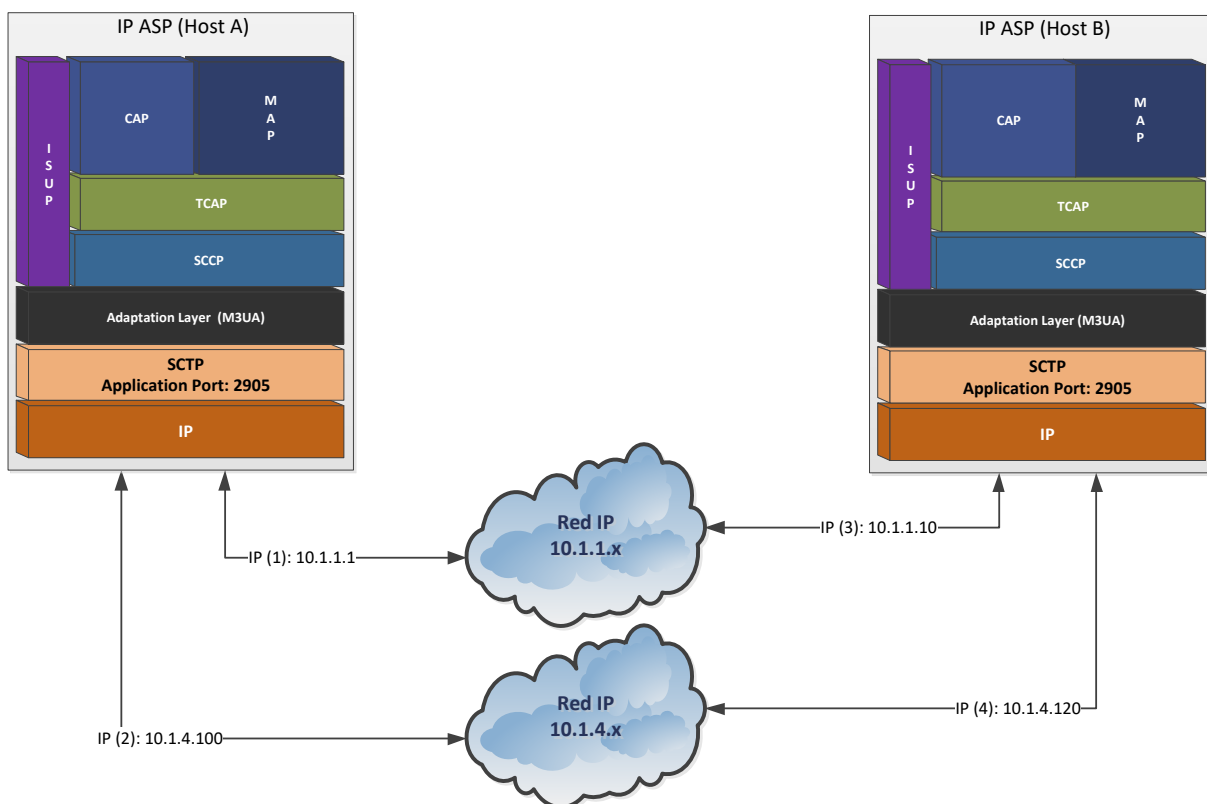


Figure A - 95. SIGTRAN Multi-homing.



During multihoming use along an SCTP association formed by two endpoints like the aforementioned example, a path is chosen as the primary meanwhile the remaining path is set as the secondary. The packets are transmitted by default by the primary path when available. At the eventuality of packet loss in the primary path, the retransmission must be done through the secondary path. Figure A-96 exposes the packet retransmission with TSN (Transmission Sequence Number) 1 on the secondary or alternative path in this example.

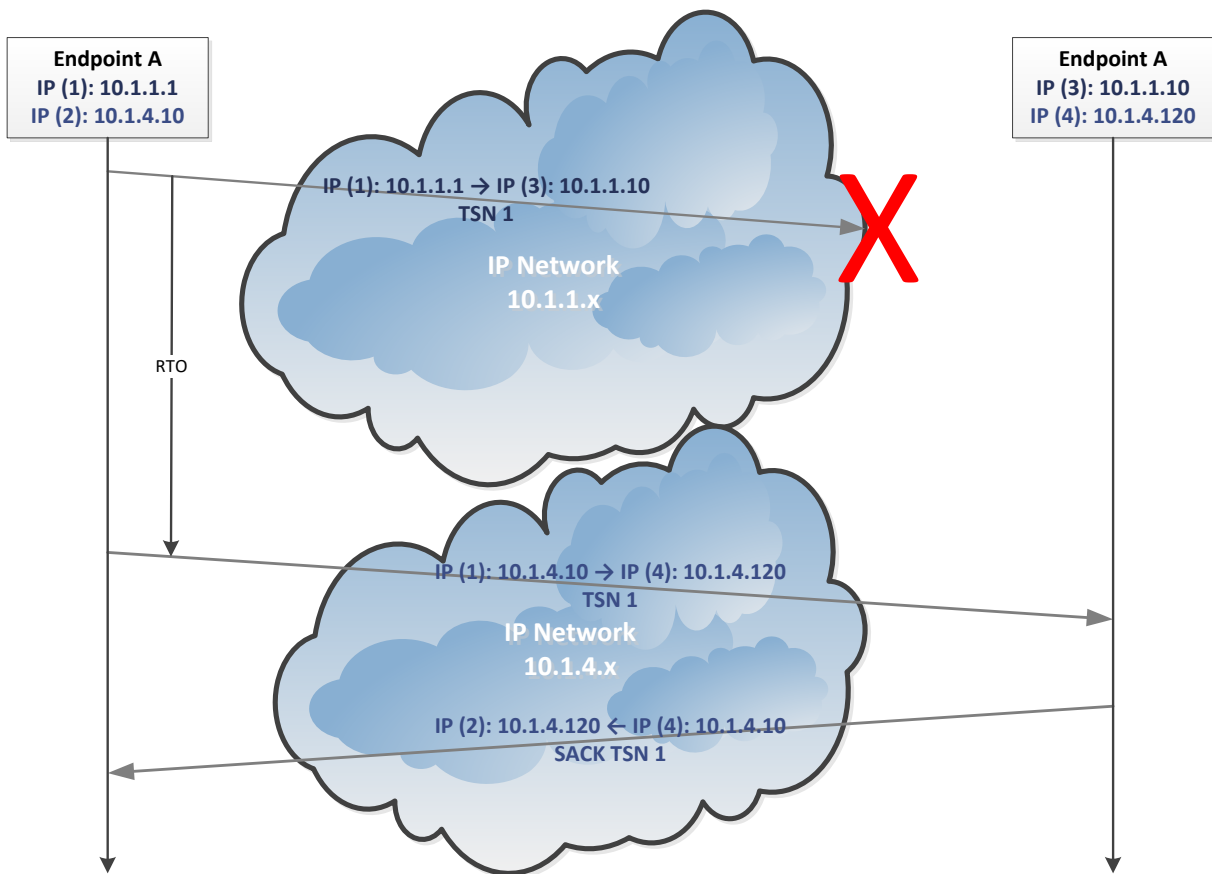


Figure A - 96. Sctp packet retransmission example in multi-homing setup.

### A.3.6.2.2 Multi-streaming

Multi-streaming refers to the capability of Sctp to transmit several independent streams of chunks in parallel. For example, transmitting web page images together with the web page text. In essence, it involves bundling several

connections into a single SCTP association, operating on messages (or chunks) rather than bytes.

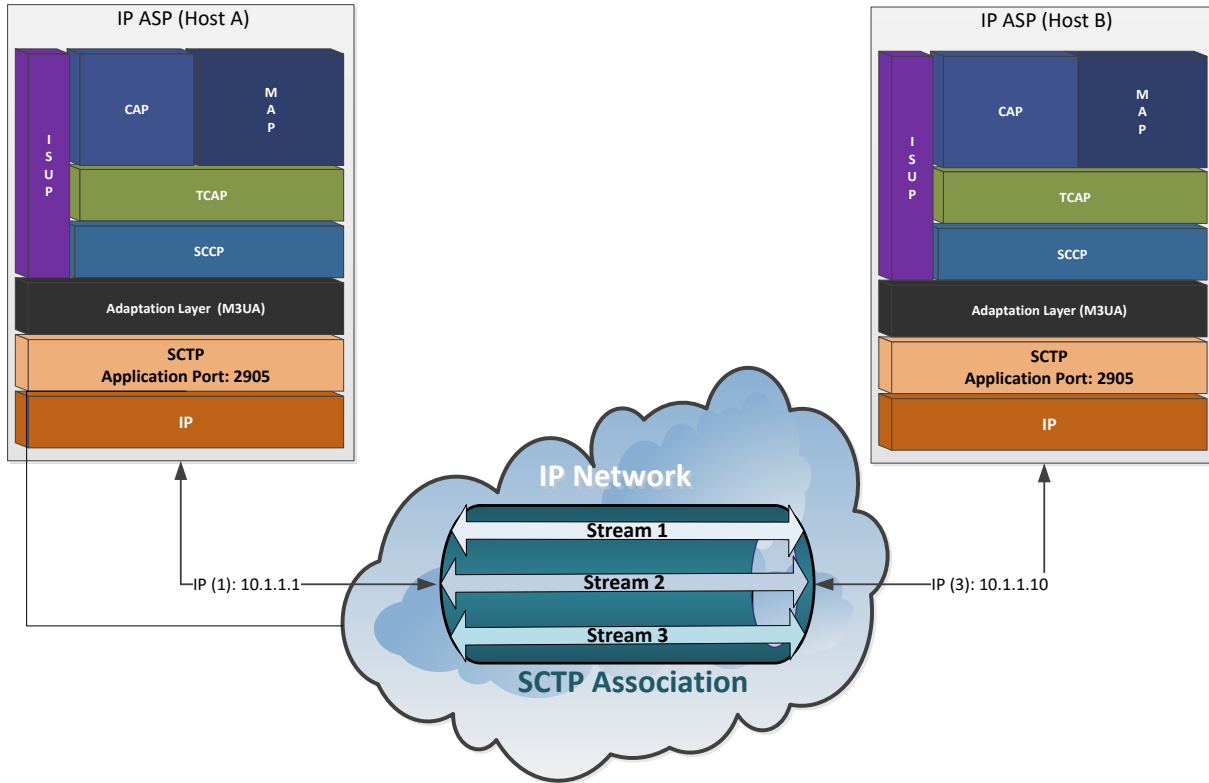


Figure A - 97. Multi-streaming within an SCTP association.

### A.3.6.2.3 SCTP datagram structure

An SCTP datagram is composed by a header and user information fragments called «chunks», as shown in the Figure A-98.

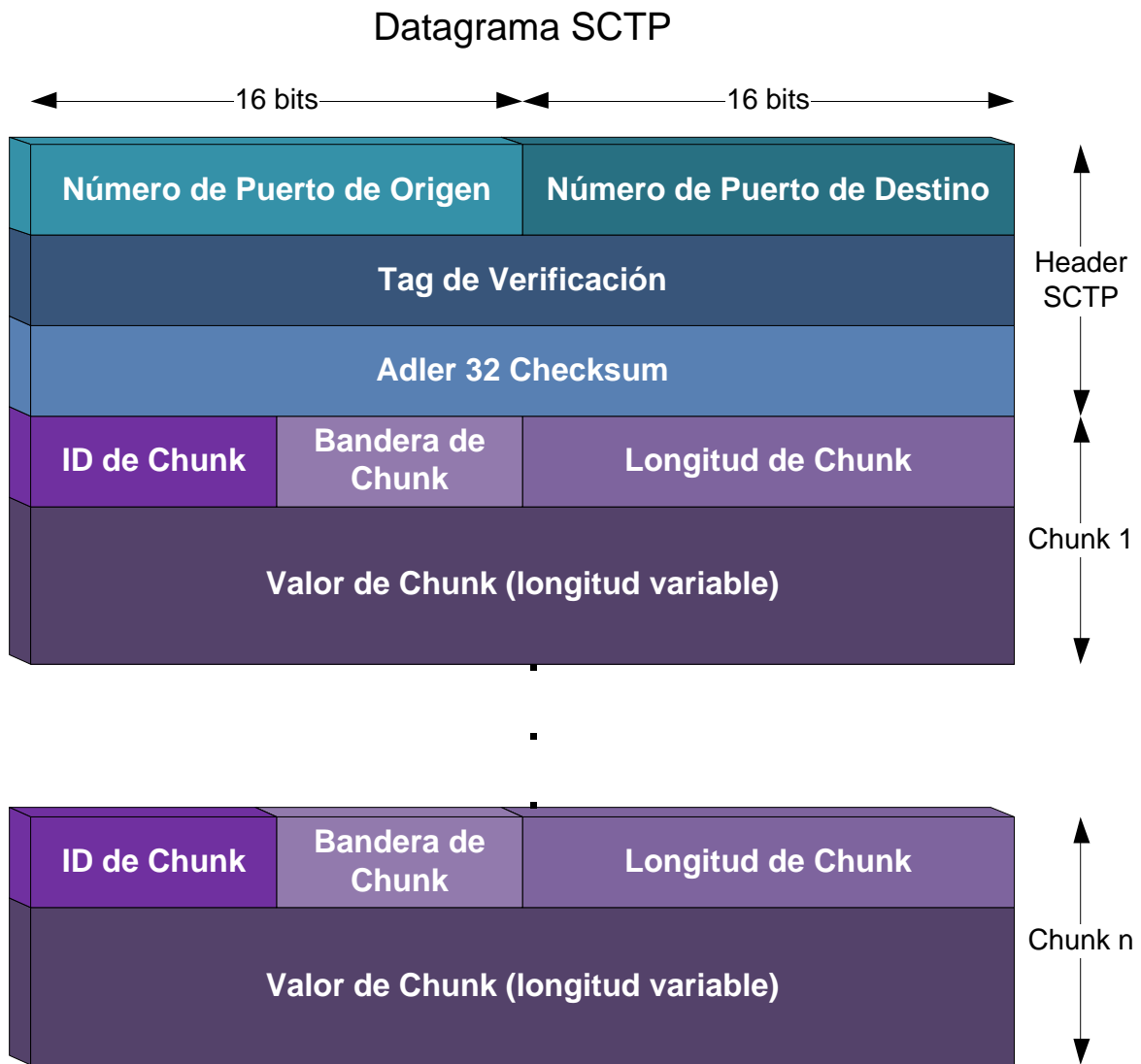


Figure A - 98. SCTP datagram structure.

SCTP datagram fields are described next:

- **Source Port Number.** Constitutes the SCTP port at the originating endpoint, coded in two octets. It might be used by the receiver for associating the datagram source by combining it with the originating IP.

- **Destination Port Number.** Constitutes the SCTP port at the destination endpoint, coded in two octets. In transmission mode, this value must be set to the tag used by the peer endpoint at the association initiation.
- **Verification Tag.** The receiving endpoint uses this tag to identify the datagram's corresponding association. In transmission mode, this value must be set to the tag used by the peer endpoint at the association initiation.
- **Adler 32 Checksum.** Constitutes an error frame verification field, by the usage of Adler 32 algorithm.
- **Chunk ID.** Indicates the type of information included at the chunk value field. It may take one of the following values:
  - 00000000            Payload Data (DATA)
  - 00000001            Initiation (INIT)
  - 00000010            Initiation Acknowledgment (INIT ACK)
  - 00000011            Selective Acknowledgment (SACK)
  - 00000100            Heartbeat Request (HEARTBEAT)
  - 00000101            Heartbeat Acknowledgment (HEARTBEAT ACK)
  - 00000110            Abort (ABORT)
  - 00000111            Shutdown (SHUTDOWN)
  - 00001000            Shutdown Acknowledgment (SHUTDOWN ACK)
  - 00001001            Operation Error (ERROR)
  - 00001010            State Cookie (COOKIE)
  - 00001011            Cookie Acknowledgment (COOKIE ACK)
  - 00001100            Reserved for Explicit Congestion Notification Echo (ECNE)
  - 00001101            Reserved for Congestion Window Reduced (CWR)
  - 00001110-11111101    Reserved by IETF
  - 11111110            Vendor-specific Chunk Extensions
  - 11111111            IETF-defined Chunk Extensions
- **Chunk Flags.** The depend on the type of used chunk. Normally, its value in one octet id zero.
- **Chunk Length.** Indicates the size of the chunk in octets, including Chunk ID, Flag, Length and Value.
- **Chunk Value.** Constitutes the information to be transferred and depends on the Chunk ID.

The different type of chunks are briefly described next:

- *Initiation (INIT)*. Used for starting an SCTP association between two endpoints, containing the following fixed/mandatory and variable/optional parameters:

<u>Fixed Parameters</u>	<u>Type</u>
Initiate Tag	Mandatory
Receiver Window Credit	Mandatory
Number of Outbound Streams	Mandatory
Number of Inbound Streams	Mandatory
Initial TSN	Mandatory
<u>Variable Parameters</u>	<u>Type</u>
IPv4 Address/Port	Optional
IPv6 Address/Port	Optional
Cookie Preservative	Optional
Reserved For ECN Capable	Optional
Host Name Address	Optional
Supported Address Types	Optional

- *Initiation Acknowledgement (INIT ACK)*. Used for sending to the remote endpoint a reception acknowledgement of the initiation of an SCTP association. Its format is almost identical to the INIT chunk, adding two extra fields: Responder Cookie and Unrecognized Parameter.
- *Selective Acknowledgement (SACK)*. Used for sending to the remote endpoint an acknowledgement of the reception of DATA chunks and inform about non-sequential data chunk reception according to TSN (Tag Sequence Number).
- *Heartbeat Request (HEARTBEAT)*. Used to inform recognition of active connection between endpoints of a specific association. It includes time values and emulates FISU in SS7.
- *Heartbeat Acknowledgement (HEARTBEAT ACK)*. Used for responding a HEARTBEAT message, so as to assuring the remote endpoint that this particular destination address of the current association is reachable. It also includes time values and emulates a FISU in SS7.

- *Abort Acknowledgement* (**ABORT**). Used to inform the remote peer of the termination of an association. This chunk may contain abort cause parameters. Data chunks are not packetized with the abort but the control chunks, although they need to be preceded by the abort in the datagram, otherwise they will be ignored.
- *Shutdown* (**SHUTDOWN**). Used by an endpoint to properly end an association with its peer endpoint.
- *Shutdown Acknowledgement* (**SHUTDOWN ACK**). Used by an endpoint to inform reception of SHUTDOWN chunk reception from the originating endpoint.
- *Operation Error* (**ERROR**). Used by an Endpoint to inform errors to its peer Endpoint within an association. It contains one or more value causes.
- *State Cookie* (**COOKIE**). Used only during the initiation of an association. It is sent by the originating Endpoint to its peer so as to completing the process. This chunk precedes any data chunk within an association, but could be embedded in one or more DATA chunks in the same datagram.
- *Cookie Acknowledgement* (**COOKIE ACK**). Used by an endpoint to inform reception of COOKIE chunk. This chunk precedes any DATA chunk within an association, but could be embedded in one or more DATA chunks in the same datagram.
- *Payload Data* (**DATA**). It contains the user's information.
- *Vendor Specific Chunk Extensions*. This type of chunk allows vendors to support their own extended data chunks, not defined by the IETF. They must not affect SCTP operation whatsoever. Those endpoints that do not understand these chunks must simply ignore them. In case an endpoint is expecting this type of chunk but is not receiving them, it must operate normally without them.

A Wireshark trace example of SCTP datagram DATA chunk is shown next.

<b>Stream Control Transmission Protocol</b> , Src Port: 4075 (4075), Dst Port: 4075 (4075)	
Source port:	4075
Destination port:	4075
Verification tag:	0x00001667
Checksum:	0xfac46887 (not verified)
DATA chunk (ordered, complete segment, TSN: 3310490045, SID: 5, SSN: 25068, PPID: 3, payload length: 148 bytes)	
Chunk type:	DATA (0)
0... .... = Bit:	Stop processing of the packet
.0.. .... = Bit:	Do not report
Chunk flags:	0x03
.... ...1 = E-Bit:	Last segment
.... ..1. = B-Bit:	First segment
.... .0.. = U-Bit:	Ordered delivery
.... 0... = I-Bit:	Possibly delay SACK
Chunk length:	164
TSN:	3310490045
Stream Identifier:	0x0005
Stream sequence number:	25068
Payload protocol identifier:	M3UA (3)

Figure A - 99. SCTP datagram DATA chunk Wireshark trace example.

### A.3.6.2.4 MTP3 User Adaptation Layer (M3UA)

IETF RFC 3332 defines the transport protocol for all type of SS7's MTPL3 user messages (SCCP, ISUP, etc.) over IP for SIGTRAN: M3UA (MTP3 User Adaptation Layer), which itself uses SCTP services. In other words, at an IP node, M3UA layer provides the set of primitives of its higher layers to MTPL3 users, likewise MTPL3 does with it local users within an SS7 node. This is done in a transparent way to the MTPL3 users in question.

M3UA is used for the communication between an SG and a MGC or an IP-resident database. The transparent transfer explained in the latter paragraph implies that the remote MTPL3 users is unaware if the service was delivered by an MTPL3 layer in an SG or by a local MTPL3 layer within an SS7 node. Likewise, the SG's MTPL3 layer is also unaware if its users are actually remote M3UA users.

A graphic interconnection diagram of how an SS7 SP connects to a network's ASP via an SG through SIGTRAN is shown next, in this case for an association using

M3UA as transport layer for SS7 MTPL3 towards IP network entities (or IP ASPs). At the SG, the MTPL3-M3UA interface is responsible for this information exchange/translation, done in a transparent way for both ends.

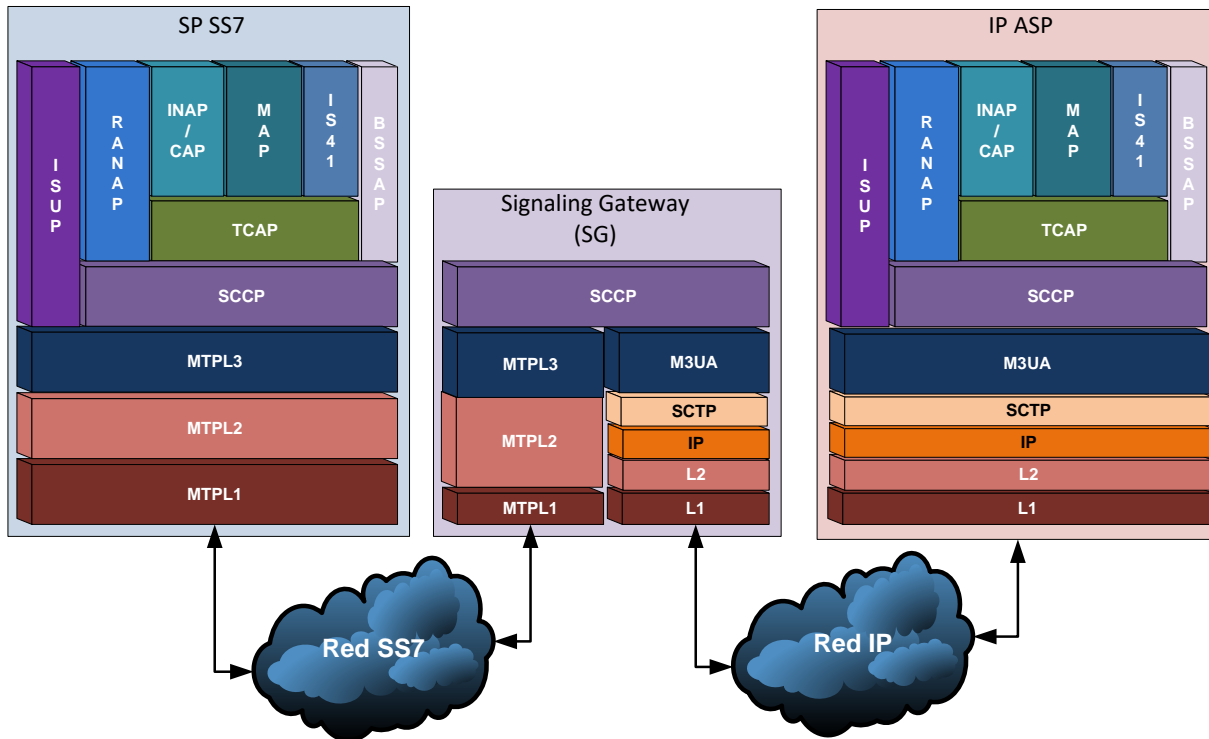


Figure A - 100. Signaling Gateway based on SCTP/M3UA.

M3UA does not impose the maximum length limitation of 272 octets for the SIF field as MTPL2 does. Broader information blocks may be included directly over SCTP/M3UA without needing segmentation/packetizing procedures like the ones specified by SCCP or ISUP. Nevertheless, the SG imposes the 272 octets limitation when connected to an SS7 network whose destination does not support transfer of larger information blocks. For High Bandwidth MTP networks, the SG fragments SCCP or ISUP messages bigger than 272 octets long, according to the correspondent needs.



**A.3.6.2.5 M3UA datagram structure**

An M3UA datagram consists of a common header, optionally/conditionally by variable length parameters according to the Message Type parameter.

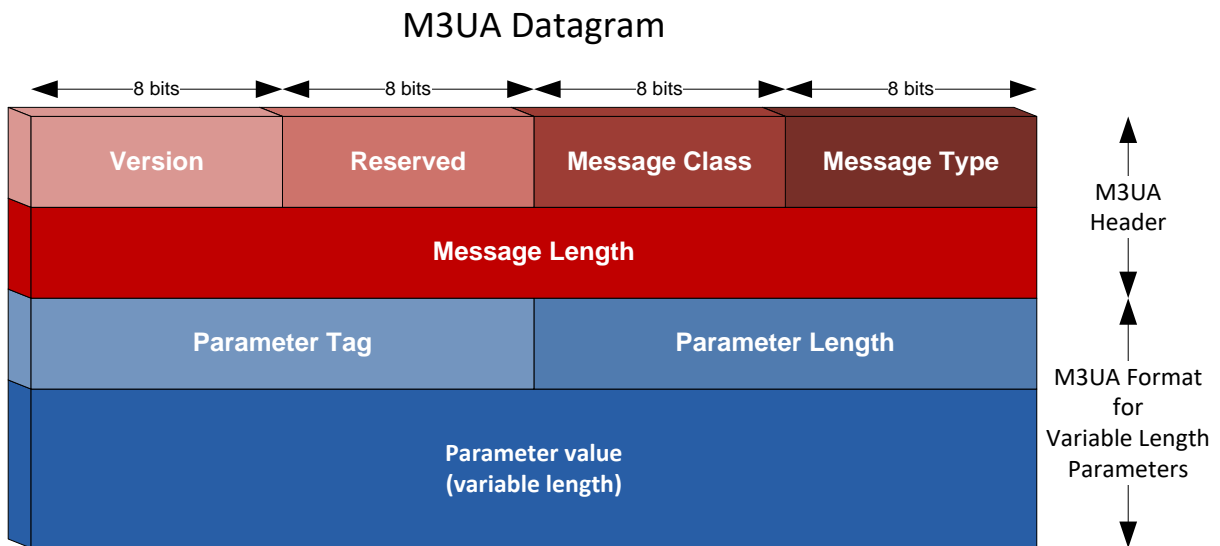


Figure A - 101. M3UA datagram structure.

M3UA datagram fields are described next:

- **Version.** This field contains the MTP3 User Adaptation Layer version.
- **Reserved.** This field is reserved for future use.
- **Message Class.** This field may contain the following values:

0	Management (MGMT)
1	Transfer Messages
2	SS7 Signalling Network Management (SSNM)
3	ASP State Maintenance (ASPSM)
4	ASP Traffic Maintenance (ASPTM)
9	Routing Key Management (RKM)

- **Message Type.** This field may contain the following values:

Management:	
0	0 Error (ERR)
1	1 Notify (NTFY)
Transfer:	
1	Payload Data (DATA)
SS7 Signalling Network Management:	
1	Destination Unavailable (DUNA)
2	Destination Available (DAVA)
3	Destination State Audit (DAUD)
4	SS7 Network Congestion State (SCON)
5	Destination User Part Unavailable (DUPU)
6	Destination Restricted (DRST)
ASP State Maintenance:	
1	ASP Up (UP)
2	ASP Down (DOWN)
3	Heartbeat (BEAT)
4	ASP Up Ack (UP ACK)
5	ASP Down Ack (DOWN ACK)
6	Heartbeat Ack (BEAT ACK)
ASP Traffic Maintenance:	
1	ASP Active (ACTIVE)
2	ASP Inactive (INACTIVE)
3	ASP Active Ack (ACTIVE ACK)
4	ASP Inactive Ack (INACTIVE ACK)
Routing Key Management:	
1	Registration Request (REG REQ)
2	Registration Response (REG RSP)
3	Deregistration Request (DEREG REQ)
4	Deregistration Response (DEREG RSP)

- **Message Length.** This field defines the message length including the header.
- **Parameter Tag.** This field indicates the type of parameter and may take one of the following values:

0	Reserved
1	Network Appearance
2	Protocol Data 1

3	Protocol Data 2
4	Info String
5	Affected Destinations
6	Routing Context
7	Diagnostic Information
8	Heartbeat Data
9	User/Cause
10	Reason
11	Traffic Mode Type
12	Error Code
13	Status Type/ID
14	Congestion Indications
15	Concerned Destination
16	Routing Key
17	Registration Result
18	De-registration Result
19	Local_Routing Key Identifier
20	Destination Point Code
21	Service Indicators
22	Subsystem Numbers
23	Originating Point Code List
24	Circuit Range
25	Registration Results
26	De-registration Results

- **Parameter Value.** This field includes the value of the parameter.

M3UA Transfer Messages (Message Class=1) contain Payload Data messages (DATA) (Message Type=1). A DATA message contains the SS7 MTP3-User protocol data, which is an MTP-TRANSFER primitive, including the complete MTP3 Routing Label.

The DATA message contains the following variable-length parameters:

- **Network Appearance** (Optional, 32 bits unsigned integer): Only of local significance, coordinated between the SG and ASP. Identifies the SS7 network context for the message and implicitly identifies the SS7 Point Code format

used, the SS7 Network Indicator value, and the MTP3 and possibly the MTP3-User protocol type/variant/version used within the specific SS7 network.

Not required if SG operates in the context of a single SS7 network, or if individual SCTP associations are dedicated to each SS7 network context. In other cases, the parameter may be configured to be present for the use of the receiver.

- **Routing Context** (Conditional, 32 bits unsigned integer): Contains the Routing Context value associated with the DATA message. Not required when a Routing Key has not been coordinated between the SG and ASP.

Where multiple «Routing Keys» and «Routing Contexts» are used across a common association, the Routing Context MUST be sent to identify the traffic flow, assisting in the internal distribution of Data messages.

- **Protocol Data** (Mandatory, variable length): contains the original SS7 MTP3 message, including the Service Information Octet (Service and Network Indicators, Message Priority), Routing Label (DPC/OPC, SLS) and User Protocol data including MTP3-user protocol elements (e.g. SCCP, ISUP, etc.)
- **Correlation ID** (Optional, 32 bits unsigned integer): uniquely identifies the MSU carried in the Protocol Data within an AS.

This Correlation Id parameter is assigned by the sending M3UA.

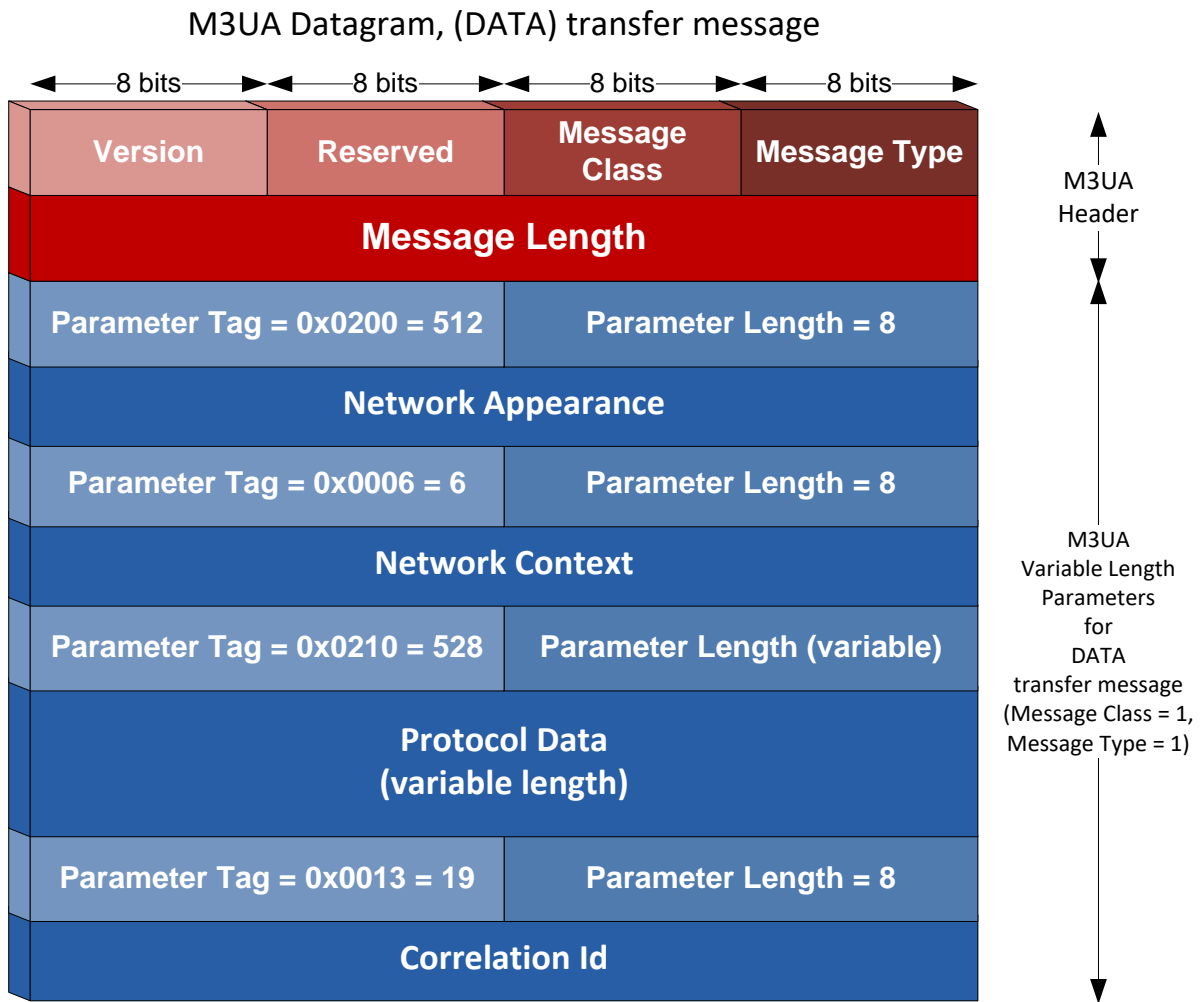


Figure A - 102. M3UA DATA message structure.

A Wireshark trace example of M3UA DATA message embedded in SCTP datagram DATA chunk is shown next.

<b>MTP 3 User Adaptation Layer</b>	
Version: Release 1 (1)	
Reserved: 0x00	
Message class: Transfer messages (1)	
Message type: Payload data (DATA) (1)	
<b>Message length: 148</b>	
Network appearance (1)	
Parameter Tag: Network appearance (512)	
Parameter length: 8	
Network appearance: 1	
Routing context (1 context)	
Parameter Tag: Routing context (6)	
Parameter length: 8	
Routing context: 1186	
Protocol data (SS7 message of 100 bytes)	
Parameter Tag: Protocol data (528)	
Parameter length: 116	
OPC: 1186	
DPC: 2178	
SI: SCCP (3)	
NI: 2	
MP: 0	
SLS: 4	
MTP3 equivalents	
OPC: 1186	
DPC: 2178	
PC: 1186	
PC: 2178	
NI: 2	
Correlation identifier (4663859)	
Parameter Tag: Correlation identifier (19)	
Parameter length: 8	
Correlation Identifier: 4663859	

Figure A - 103. M3UA message Wireshark trace example.

## **Annex B**

### **B Global System for Mobile (GSM)**

#### **B.1 Introduction**

By 1982, the European Conference of Postal and Telecommunications Administrations (CEPT), creates GSM («Groupe Spécial Mobile», later renamed to «Global System for Mobile»). The objective was creating a single European standard mobile system compatible with existent and future services over the already initiated ISDN project.

GSM turned out being the most successful second generation mobile communications system still being up to date the one with most subscriptions and wireless coverage worldwide according to [10], regardless of relentless technology advance towards 3G/4G/5G. Obviously, this scenario is changing, but as can be seen in Figure B.1, by 2021 there will be more than 1 billion GSM-only subscribers worldwide.

This annex purpose is providing a high-level overview of GSM/GPRS/EDGE main network components and interfaces. As an SS7 based network, some of the high level view is already covered there and both annexes turn out be complimentary of each other, as well as consistent with the concepts addressed in the main chapters of this work. Further details are beyond the scope of this work.

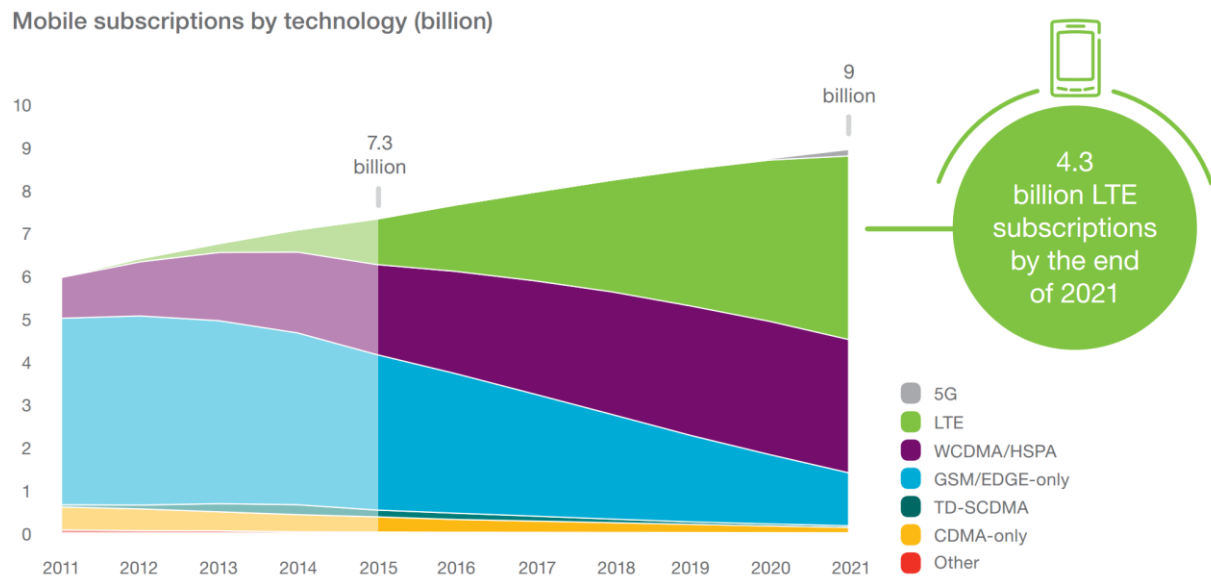


Figure B - 1. Mobile subscriptions by technology [10].

## B.2 GSM Network Architecture

GSM network architecture is composed of the following basic subsystems, performing the detailed main functions:

- NSS (Network Subsystem)
- Base Station Subsystem (BSS)
- Network Management Subsystem (NMS)

Together, these subsystems compose a GSM PLMN (Public Land Mobile Network) which also connects other PLMNs or telephony systems like the PSTN (Public Switched Telephone Network), ISDN (Integrated Services Digital Network), etc.

### B.2.1 Base Station Subsystem (BSS)

GSM's Network Subsystem main responsibilities encompass the following:

- Traffic and signaling management between the mobile users and NSS.
- Transcoding of voice channels.



- Radio channels assignment.
- Paging for service provisioning.

GSM' BSS entities are briefly described next.

- MS (Mobile Station): a GSM mobile station is divided in two main parts:
  - Mobile Equipment (ME): Hardware and Software needed for the Man-Machine-Interface (MMI)
  - SIM (Subscriber Mobile Identity): comprises an intelligent or logical card acquired when subscribing to a GSM network. It is introduced in the MS and associates it with the user. SIM card possesses an amount of identities among which the following are highlighted:
    - IMSI (International Mobile Subscriber Identity), used for identifying a subscriber during several processes across the network such as location update, terminating call, roaming charging, etc. It consists of a number of maximum 15 digits, divided in MCC (Mobile Country Code) and MNC (Mobile Network Code), both specified by ITU-T E.212, and the MSIN (Mobile Subscriber Identity Number) which identifies a subscriber within the PLMN.

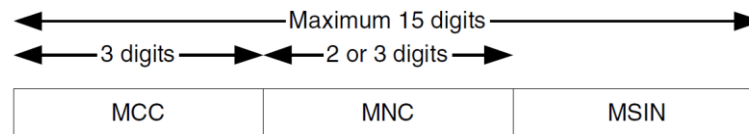


Figure B - 2. IMSI structure.

- Ki (Authentication Key), only stored by the HLR and MS.
- Kc (Cryptography Key), result of A3/A8 algorithm, Ki, and random number (RAND).
- TMSI (Temporal Mobile Subscriber Identity): assigned temporarily by the VLR in replacement of the IMSI for security measures.

The MS is identified by most users through the MSISDN (Mobile Subscriber Integrated Services Digital Network Number), which is a directory number composed of the following: MSISDN = CC (Country Code) + NDC (National Destination Code) + SN (Subscriber Number) (ITU-T Rec. E.164, §6.2.1).

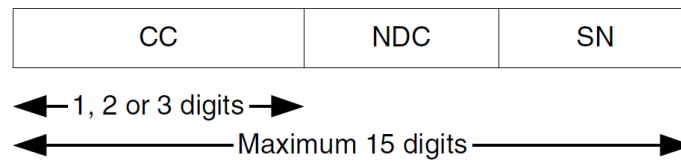


Figure B - 3. MSISDN structure.

- **BTS (Base Transceiver Station).** Constitutes the transmitter/receiver devices, including antennas and signal processing units needed for the radio interface. It covers a unit known as cell, usually divided in three 120° sectors. The BTS usually contains the TRAU (Transcoding and Rate Adaptation Unit), where coding/decoding of GSM specific voice is done, providing an interface between PCM A-law and GSM codec, as well as bit rate adaptation for data channels.
- **BSC (Base Station Controller).** All BTSs giving radio coverage to a specific geographic area are connected to a BSC through the Abis interface. BSC roles include all BSS main functions, namely: RF channel connection establishment and release, power control, handoff or handover, paging, authentication, etc.

### B.2.1.1 GSM Logical Channels

GSM radio interfaces uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access).

In FDMA, each user is assigned with a particular frequency or carrier. In TDMA, each user is assigned with time slot to transmit information, then increasing the capacity of analogue channels (in GSM each carrier supports 8 time slots -TS-).

Each cell supports multiple carriers, while for each carrier 8 TS are located, which may transport several types of information bursts.

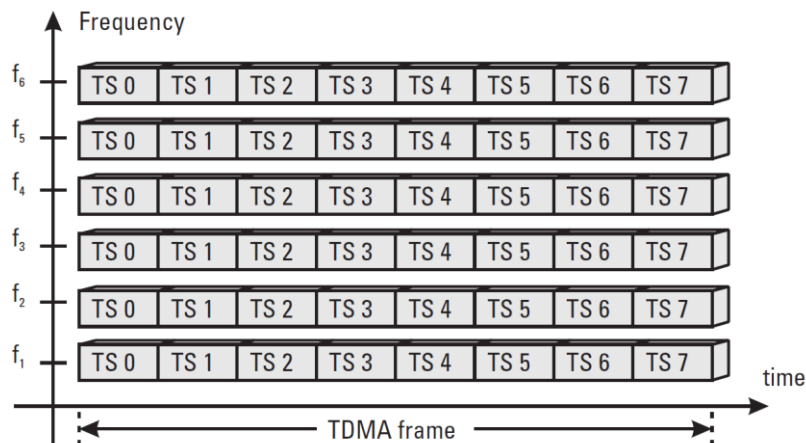


Figure B - 4. FDMA/TDMA structure of GSM [14].

Between the user and the network, two types of logical channels are defined for GSM/UMTS radio access:

- **Control channels** (for the transfer of control plane information), categorized as Half Rate (5.6kbps), Full Rate (13kbps) and Enhanced Full Rate (13 kbps) bidirectional channels.
  - Broadcast Control Channel (BCCH): downlink channel for broadcasting system control information.
    - Synchronisation Channel (SCH): used to identify the BTS and frame synchronization.
    - Frequency Correction Channel (FCCH): data burst in the TS0 repeated every 10 frames. Used for frequency correction at the MS.
    - Broadcast Control Channel (BCCH): sends the Cell Global Identity (CGI) and Location Area Identity (LAI) cell operation characteristics and neighbour cells list.
  - Paging Control Channel (PCCH): downlink channel for transferring paging information. This channel is used when the network does not know the location cell of the MS/UE, or, the MS/UE is in the cell connected state (using sleep mode procedures).
  - Common Control Channel (CCCH): Bi-directional channel for transmitting control information between network and UEs. This channel is commonly used by the MS/UEs having no RRC (Radio Resource Control) connection with the network and by the MS/UEs using common transport channels when accessing a new cell after handoff/handover.

- Paging Channel (PCH): sends messages to all neighbour cells for acknowledging call requests.
  - Random Access Channel (RACH): used for requesting a call or responding an alert in the uplink direction.
  - Access Grant Channel (AGCH): provides instructions to the MS for operating in a specific channel. Used by the BTS to answer a RACH message.
  - Dedicated Control Channel (DCCH): point-to-point bi-directional channel that transmits dedicated control information between a MS/UE and the network. This channel is established through RRC connection setup procedure.
    - Standalone DCCH (SDCCH): Transports authentication and alert messages previous to traffic channel assignment. Also used for messaging service like USSD and SMS in the air interface.
    - Slow Associated Control Channel (SACCH): always associated to the traffic channel assigned to the MS. BTS sends power and synchronism instructions, while the MS uses it for providing information on the air channel's quality.
    - Fast Associated Control Channel (FACCH): transport urgent messages like the ones needed for handoff/handover.
  - Shared Channel Control Channel (SHCCH): Bi-directional channel that transmits control information for uplink and downlink shared channels between network and MS/UEs. This channel is for TDD only.
  - MBMS point-to-multipoint Control Channel (MCCH): A point-to-multipoint downlink channel used for transmitting control information from the network to the UE. This channel is only used by MS/UEs that receive MBMS.
  - MBMS point-to-multipoint Scheduling Channel (MSCH): point-to-multipoint downlink channel used for transmitting scheduling control information, from the network to the MS/UE, for one or several MTCHs carried on a CCTrCH. This channel is only used by UEs that receive MBMS.
- **Traffic channels** (for the transfer of user plane information), further classified as Broadcast, Common and Dedicated Control channels.

- **Dedicated Traffic Channel (DTCH):** Dedicated Traffic Channel (DTCH) is a point-to-point channel, dedicated to one MS/UE, for the transfer of user information. A DTCH can exist in both uplink and downlink.
- **Common Traffic Channel (CTCH):** point-to-multipoint unidirectional channel for transfer of dedicated user information for all or a group of specified UEs.
- **MBMS point-to-multipoint Traffic Channel (MTCH):** point-to-multipoint downlink channel used for transmitting traffic data from the network to the UE. This channel is only used for MBMS.

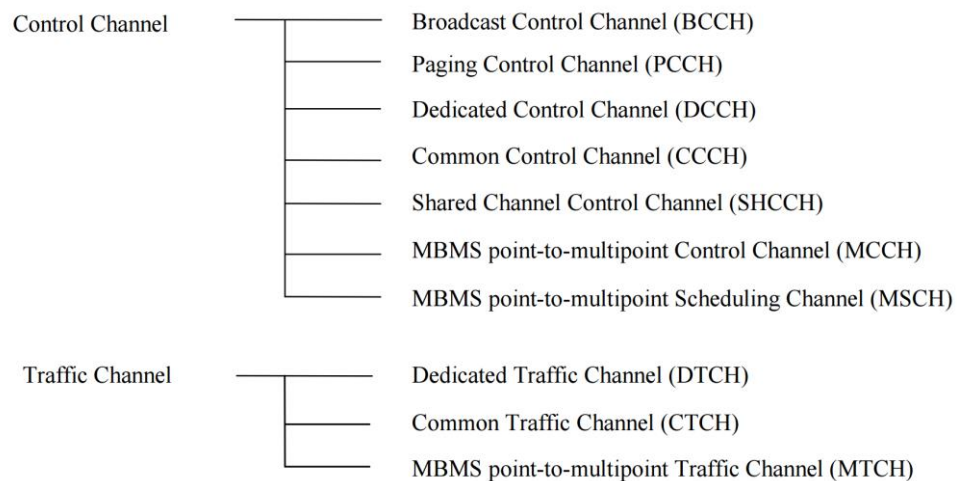


Figure B - 5. GSM Logical channel structure [E1].

### B.2.2 Network Subsystem (NSS)

GSM's Network Subsystem main responsibilities encompass the following:

- Switching capability either between mobile-mobile or mobile-fixed lines.
- User profile management.
- Mobility management.

GSM' NSS entities are briefly described next.

- MSC (Mobile Switching Centre): core network main switching entity. All subscribers under GSM radio access are attached at the GSM, registered under its own database (VLR). All incoming and outgoing calls from/to these subscribers are controlled by the MSC they are attached to. MSC are geographically distributed to distributing GSM coverage across the PLMN, which may have one or more MSC geographically distributed.
- VLR (Visitor Location Register): contains the current subscriber's information of the subscribers attached at the MSC at a specific moment (including CAMEL Subscription Information obtained from the HLR). Even though MSC and VLR are accessible as unique entities, they compose an integrated system (discriminated in SS7 by the Subsystem Number -while SSN 8 is assigned to the MSC, SSN 7 is assigned to the VLR).
- GMSC (Gateway MSC): comprises a switching node for handling mobile terminated calls, acting as a gateway between the mobile subscriber and the calling party's network (PSTN, other PLMN, etc.). When a call is established with a GSM subscriber, the GMSC contacts the subscriber's home HLR so as to gathering the MSC/VLR address where is actually attached to. This information is used for routing calls to the target destination.
- HLR (Home Location Register): encompasses the database containing all records of each subscriber of the Home PLMN (H-PLMN). The MSISDN is provisioned at the HLR as part of the subscriber's profile and is sent to the MSC during the registration stage to the MSC or an SCP at CAMEL invocation service. The HLR is responsible for sending data to the VLR during the registration phase, or towards the GMSC (during call management or termination).
- AuC (Authentication Centre): The AuC is addressed by the HLR to determine if the MS shall be provided with service. It defines if the MS is authentic by sending an encrypted message and verifying the mobile's response. Authentication is then based on the signaling messages exchanged between the AuC and the subscriber's SIM card. The method is based on the random number sequence known as RAND, the authentication key ( $K_i$ ) only stored at

the SIM and AuC and unique per each subscriber, and an algorithm (A3 or A8) which calculates a response from RAND and  $K_i$ .

- EIR (Equipment Identity Register): database which keeps records of legit, fraud and failed MSs (models, software, versions, blacklists, etc.). For this purpose, it uses the «International Mobile Equipment Identity» (IMEI), used to identify the MS's ME, having each ME a unique IMEI. The IMEI is encoded as an eight bytes' string as specified by GSM TS 03.03, containing type approval code (TAC), final assembly code (FAC) and serial number (SNR) (in CAMEL phase 4, Software Version or SV is introduced as part of the IMEI or IMEISV).

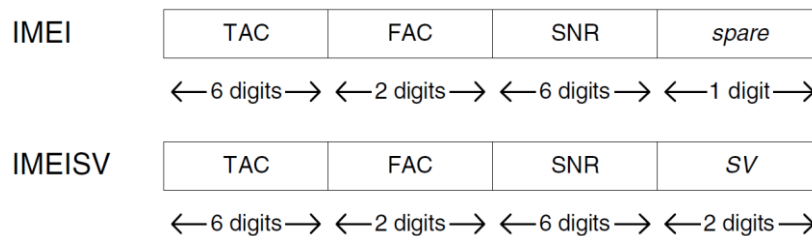


Figure B - 6. IMEI and IMEISV structure.

### B.2.3 Network Management Subsystem (NMS)

GSM Network Management Subsystem provides monitoring, controlling, configuring, maintaining and managing capabilities of GSM network elements. GSM' NMS entities are briefly described next.

- **NMC** (Network Management Center): manages all the network: high level alarm monitoring, overload control, traffic control, planning, etc. It may replace an OMC
- **OMC** (Operation and Maintenance Center): typically, responsible of a subsystem (BSS or NSS). Supervises the network's state, manages alarms, performance, configuration control, traffic information collection, etc.
- **ADC** (Administration Centre): responsible of network administrative functions such as user's subscriptions and billing.

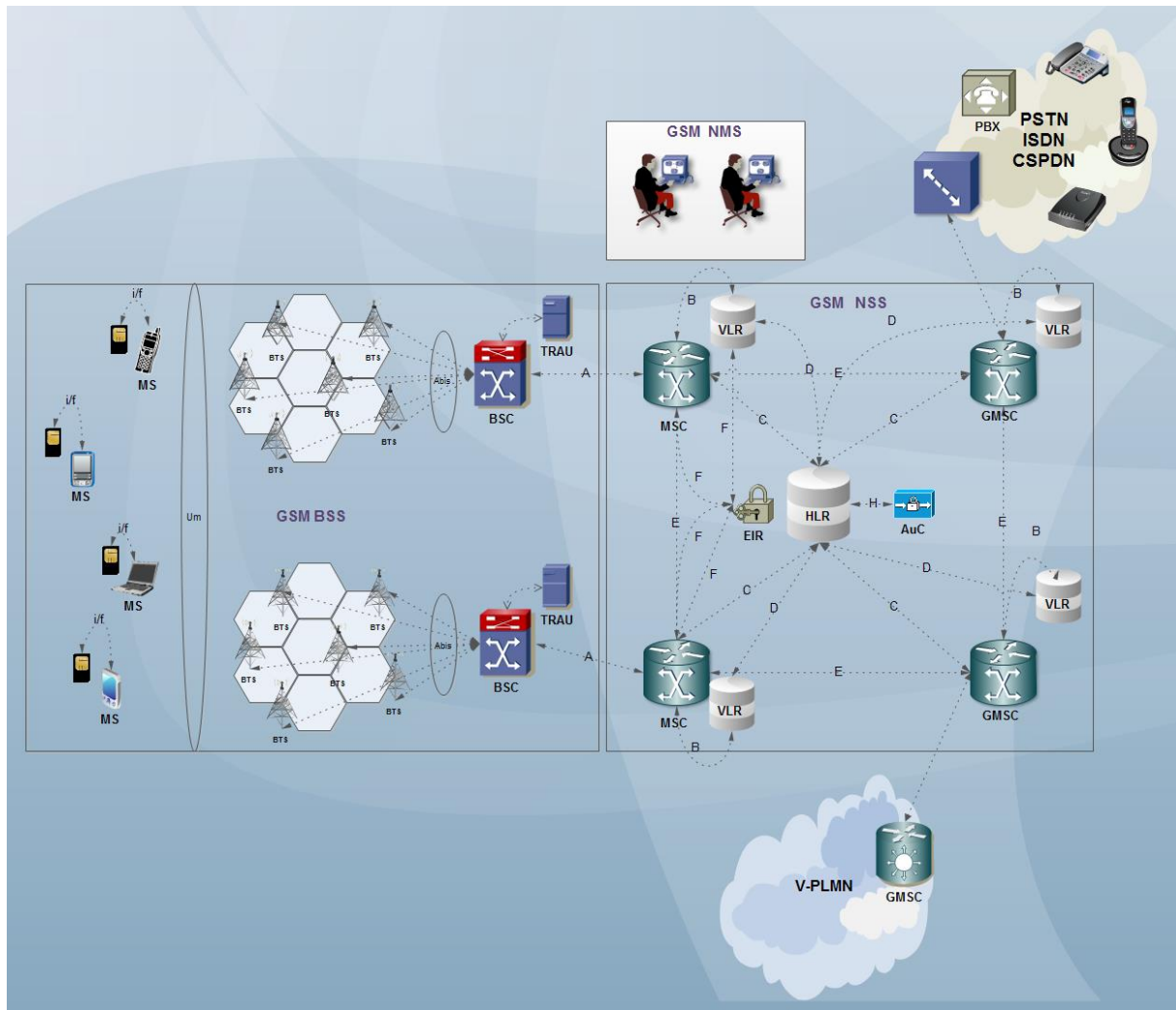


Figure B - 7. GSM network subsystems and main entities overview.

### B.2.3.1 GSM Registration, Authentication and Location procedure

This section will briefly describe the procedures done in a GSM network when a user turns on a mobile station. The steps followed are the following:

- The user turns on the MS.
- The MS selects the carrier with perceived higher power.
- The MS syncs with the BTS through FCHH and SCH.
- The MS retrieves LAI.
- If LAI differs from previous one at the SIM, a location update is begun.



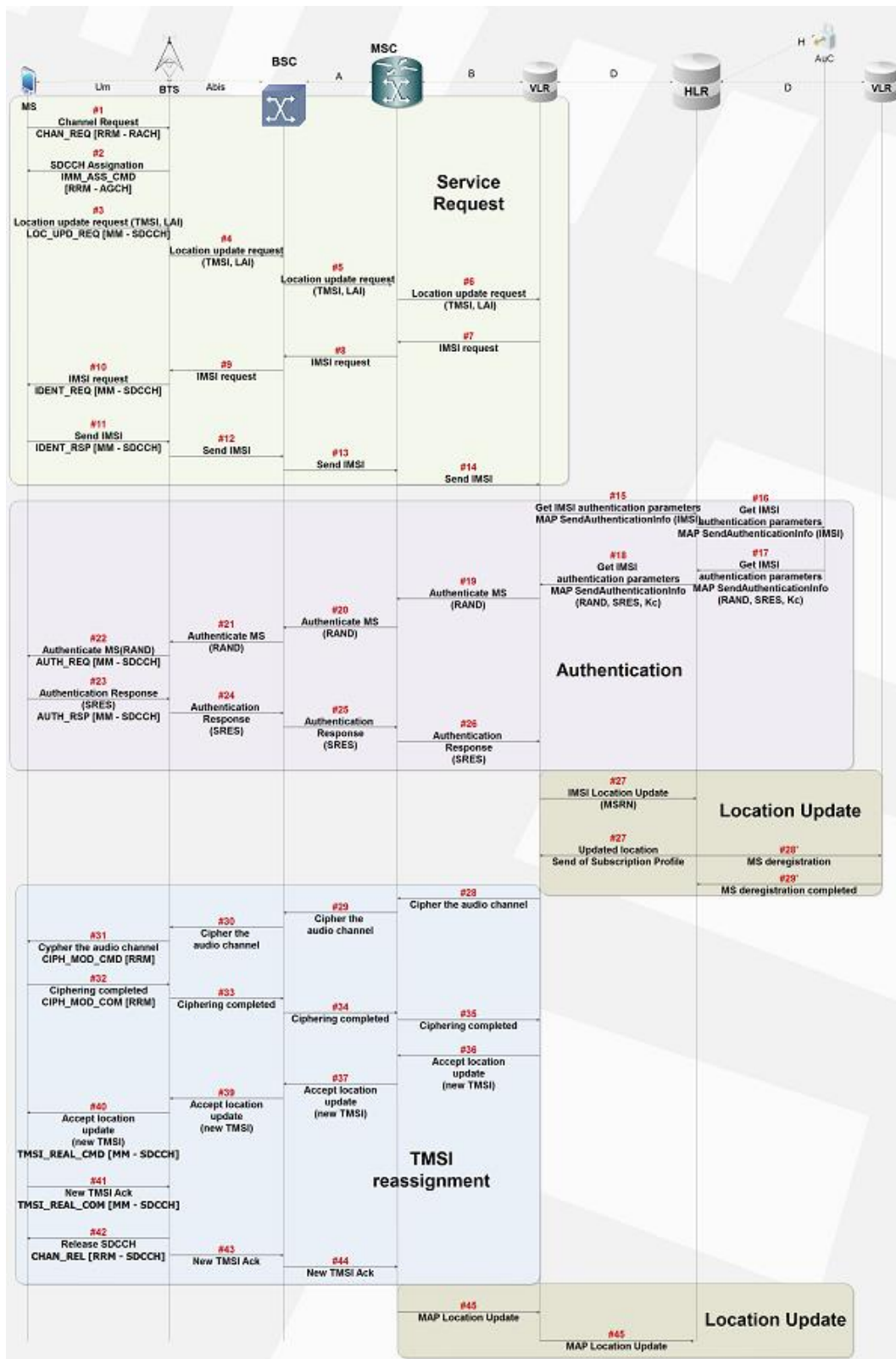


Figure B - 8. GSM registration, authentication and location update procedures.

### B.2.3.2 Basic Call Establishment

After service registration, authentication, TMSI reassignment and location update procedures as displayed in previous call flow, the MS is able to send/receive calls. Next diagram and following explanation describes the steps for such basic service (call establishment within a mobile network either mobile originated or mobile terminated). Diagram below only depicts basic operations for call establishment (no CAMEL call control involved).

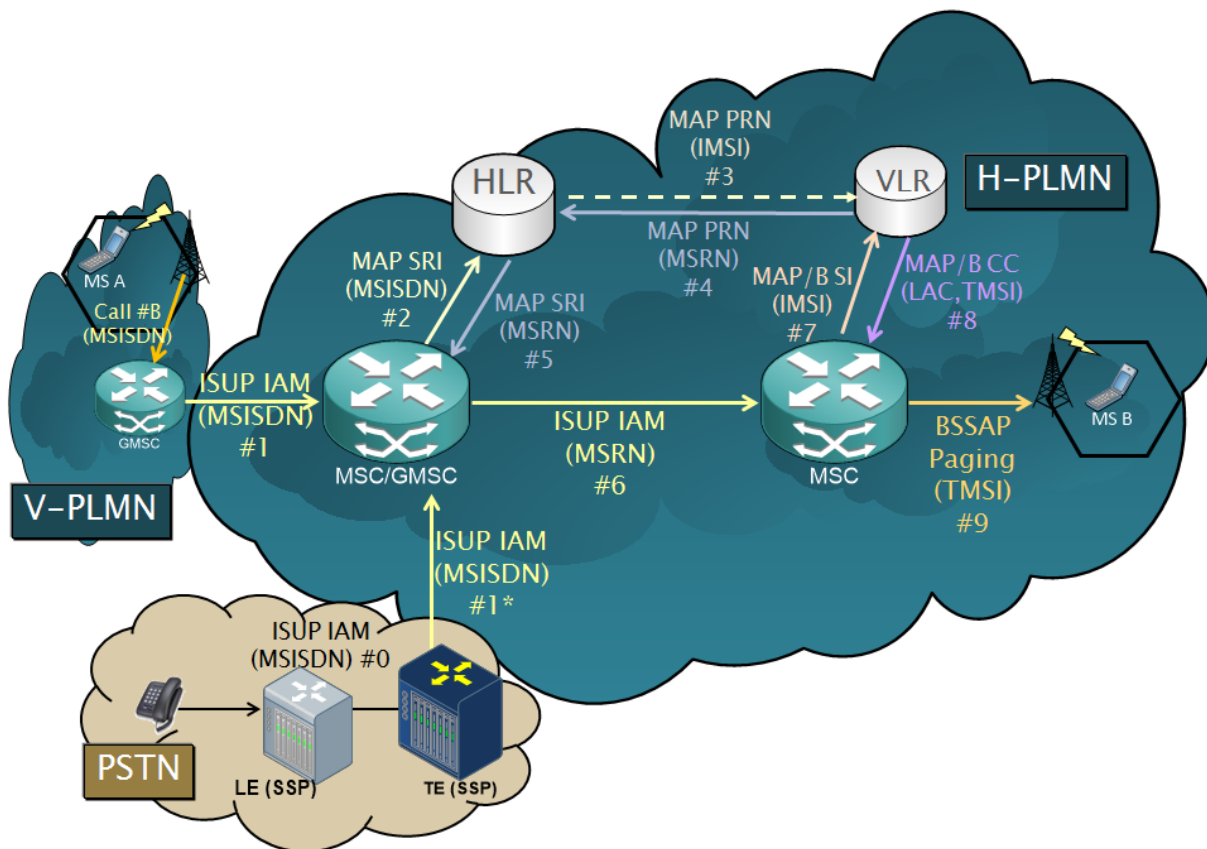


Figure B - 9. Simple mobile originated/terminated call establishment in GSM.

Previous call flow diagram is described next:

0. MS A calls MS B roaming in a V-PLMN (Visited-PLMN).
1. GMSC forwards ISUP IAM to H-PLMN with MSISDN in called party address. (0\* and 1\* emulates 0 and 1 but from the PSTN)
2. GMSC sends a MAP SRI operation request to the HLR, for acquiring routing information for the call.

3. HLR sends PRN request to the VLR at where B party is attached to (identified by the MSISDN), in order to acquire current MSRN (Mobile Subscriber Roaming Number).
4. VLR send back the MSRN in PRN response to the HLR.
5. HLR sends back the routing information to the GMSC with PSRN, in order to continue the call and forward the ISUP IAM to the proper destination and using adequate current roaming number.
6. GMSC forward ISUP IAM to the MSC/VLR at where B party is attached to, identified by MSRN instead of MSISDN.
7. MSC requests LAC and TMSI from the VLR in order to send the call to the Radio Access Network.
8. VLR sends back the LAC and TMSI of the B party to the MSC.
9. MSC sends a paging request in BSSAP to the BSC/BTS/MS. Then, after MS is paged, rest of normal ISUP call progresses as described in annex A.

### **B.3 GPRS/EDGE Network Architecture**

First steps towards telecommunications services convergence in GSM mobile networks was the deployment of General Packet Radio Services (GPRS), as specified by 3GPP TS 23.060 [E2]. GPRS commitments covered the following main items:

- Data transmission/reception from/to multi-protocol networks.
- Use of pre-existing cellular network infrastructure.
- Mobility.
- Wider coverage.
- No interference with voice service.

Three operation modes were initially defined for GPRS:

- A mode: the MS receives GSM services (e.g. voice, SMS, etc.) and GPRS data services simultaneously with no service interruption whatsoever.
- B mode: the MS might be attached to either networks (GSM or GPRS), but only have one active connection.
- C mode: the MS shall only be connected to one of the networks (mostly used by GPRS modems).

GSM network element	Adjustment or update for GPRS
User Equipment	A complete new terminal is required to access either GPRS data services and GSM voice calls
BTS	A software update is needed.
BSC	A software update is required, as well as a new equipment called PCU (Packet Control Unit) for routing traffic towards the GPRS Packet-Switched Core Network.
Core Network	Two new nodes are required for composing the GPRS Packet-Switched Core Network: <b>SGSN</b> ( <i>Serving GPRS Support Node</i> ) y <b>GGSN</b> ( <i>Gateway GPRS Support Node</i> )
Databases (HLR, VLR, etc.)	All of them require updates for adapting to new state models and methods introduced by GPRS.

Table B - 1. Update of the GSM network for GPRS deployment.

GPRS introduces two additional nodes for composing the GPRS Packet Switched Core Network (PS CN), through which an MS may establish a connection with a PDN -Packet Data Network- (e.g. Internet), namely:

- **SGSN (Serving GPRS Support Node)**. The SGSN keeps location/mobility tracking of the MS at the same time it carries out functions regarding security, access control, online charging/billing (normally through a CAMEL relationship with an SCP). It connects to the access network (later renamed to GERAN as for GPRS EDGE RAN) through the G<sub>b</sub> interface with the BSC. Other core network entities use the SGSN for SMS submission, i.e. SMSC' IW MSC and SMS GMSC. In summary, it sends and receives data packets from the mobile stations and manages the following functions along with GSM entities support (i.e. HLR, (G)MSC/VLR, AuC, EIR, etc.):
  - Authentication.
  - Registration.
  - Access control.
  - Mobility.
  - Gathering of RAN usage charging/billing information.

- **GGSN (Gateway GPRS Support Node).** Acts as a router providing an interface with other databases or PDNs, and is connected to Core Network entities within an IP domain. The GGSN stores routing information of registered mobile stations. It also collects rating information of external networks usage for AAA (Authentication, Authorization and Accounting) through RADIUS or Diameter interfaces.

Although GPRS provided Internet access to the mobile subscriber, the solution didn't turn out being optimal. Consequently, EDGE (Enhanced Data for GSM Evolution) technology is introduced, whose objective was improving data transfer rate. EDGE introduces the following upgrades:

- New packet coding methods of the new introduced transmission channels, as well as a new modulation scheme transition from GMSK (Gaussian Minimum Shift Keying) to 8-PSK (8-Phase Shift Keying), thus in theory data rates reaches 384 Kbps.
- BSS (Base Station Subsystem) adopts a new name, i.e. GERAN (GSM EDGE Radio Access Network). Although achieving a higher data transfer rate, a cost was introduced as more BTSs were needed for achieving such goal.

GPRS/EDGE also introduces the following capabilities:

- *Control:* GTP (GPRS Tunneling Protocol) is the IP based protocol used between GPRS nodes. When the MS requests a GPRS session begin, the SSN establishes a tunnel known as PDP Context (Packet Data Protocol Context) from the new IP/ATM backbone access network (GERAN) towards the GGSN. All control traffic and data pass through this tunnel.
- *Security:* the user is authenticated at the SGSN according to the subscription information retrieved from the HLR.
- *QoS (Quality of Service):* quality of service is negotiated during PDPc establishment.
- *Mobility:* the SGSN keeps track of the MS location jointly with the GERAN.
- *Charging:* the SGSN generates charging/billing information either on Kbytes or time. This information is often shared with an Online/Offline Charging System through CAP. The GGSN also generates charging/billing information, often shared with a Charging Gateway or AAA system via RADIUS or Diameter protocols.

Following diagram depicts a basic scheme of a GSM network with the addition of a GPRS/EDGE Packet-Switched Core Network.

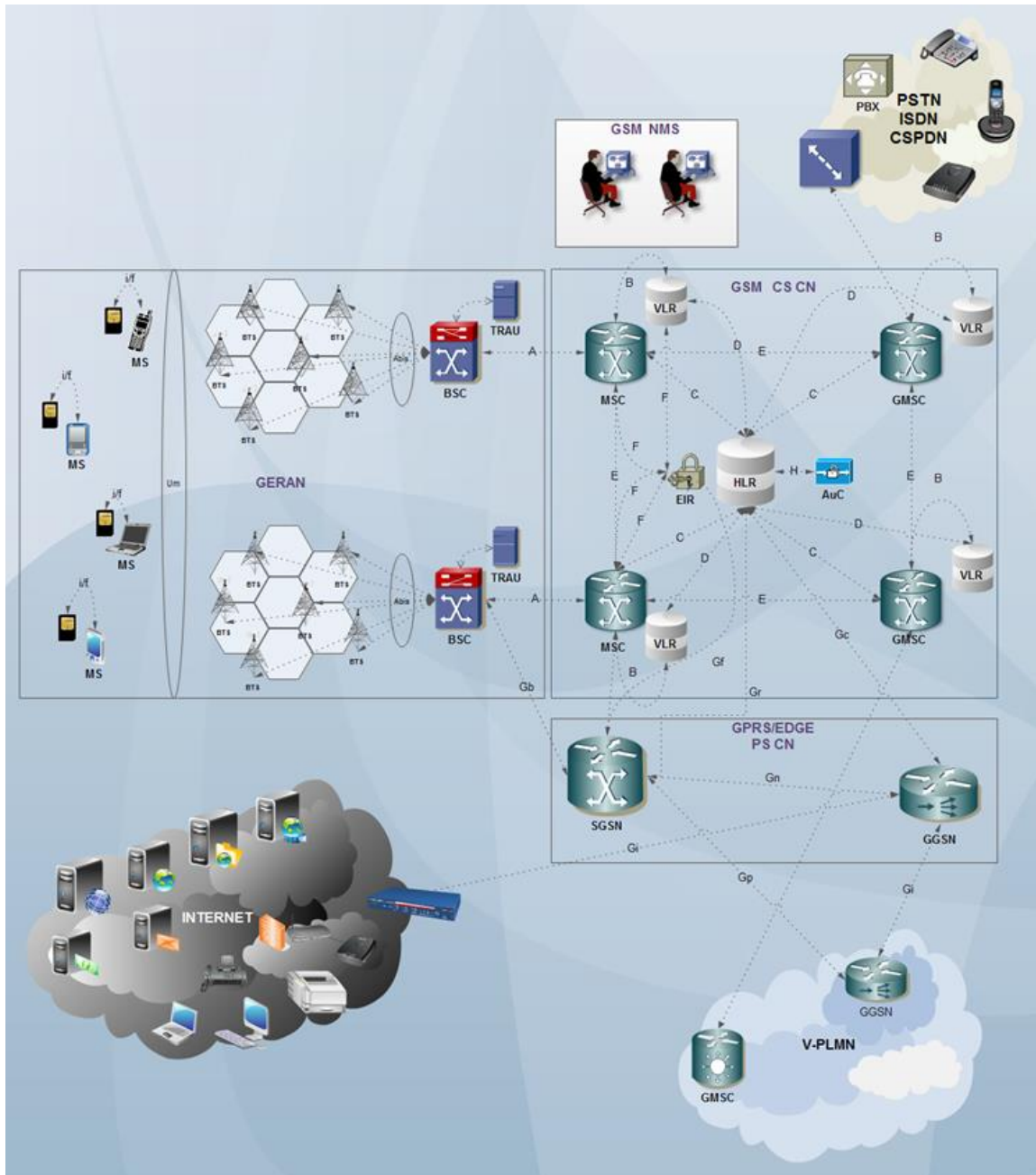


Figure B - 10. GSM and GPRS/EDGE basic network overview.

## Annex C

### C UMTS and NGN

#### C.1 Introduction to UMTS

Since 1985 work groups were gathered by ITU for solving mobile telecommunications limitations. Briefly, next aims were established:

- High degree of global scale design homogeneousness.
- Worldwide roaming.
- Multimedia applications capacity for a wide range of services and terminals (e.g. videoconference, high speed Internet, high definition voice and data, up to 2 Mbps data transfer).

This works converged IMT-2000 (International Mobile Telecommunications-2000), created as the global standard for third generation mobile communications. IMT-2000 is then the collaboration outcome of different standards groups and aims at providing telecommunications services access using radio links, including terrestrial and satellite networks. IMT-2000 ensue 3GPP (Third Generation Partnership Project) and 3GPP2 (Third Generation Partnership Project 2) standards. Their technical specifications arise by 1988 via the collaboration of all the main players in the telecommunications industry, namely:

- ETSI (European Telecommunications Standards Institute)
- Japan's ARIB (Association of Radio Industries and Business)
- CCSA (China Communications Standards Association)
- United States of America T1 Committee
- South Korea's TTA (Telecommunications Technology Association)
- Japan's TTC (Telecommunications Technology Committee)

Meanwhile 3GPP comprises a set of technical specifications and reports (TS - Technical Specifications; TR - Technical Reports) for the third-generation mobile

telephony system known as UMTS (Universal Mobile Telecommunications System) based on the dominant second generation digital system worldwide to date, i.e. GSM, 3GPP2 surges for the evolution of North American and Asian standards based on ANSI/TIA/EIA-41 and cdma2000 towards a third generation system. 3GPP2 organization partners are the same of those of 3GPP with the addition of TIA (Telecommunications Industry Association). Besides, other 3GPP/3GPP2 partners result from the need of different markets convergence. This partners include, among other, the UMTS Forum, 3G Americas, GSMA, OMA, TISPAN, TD-SCDMA Forum, IPv6, etc.

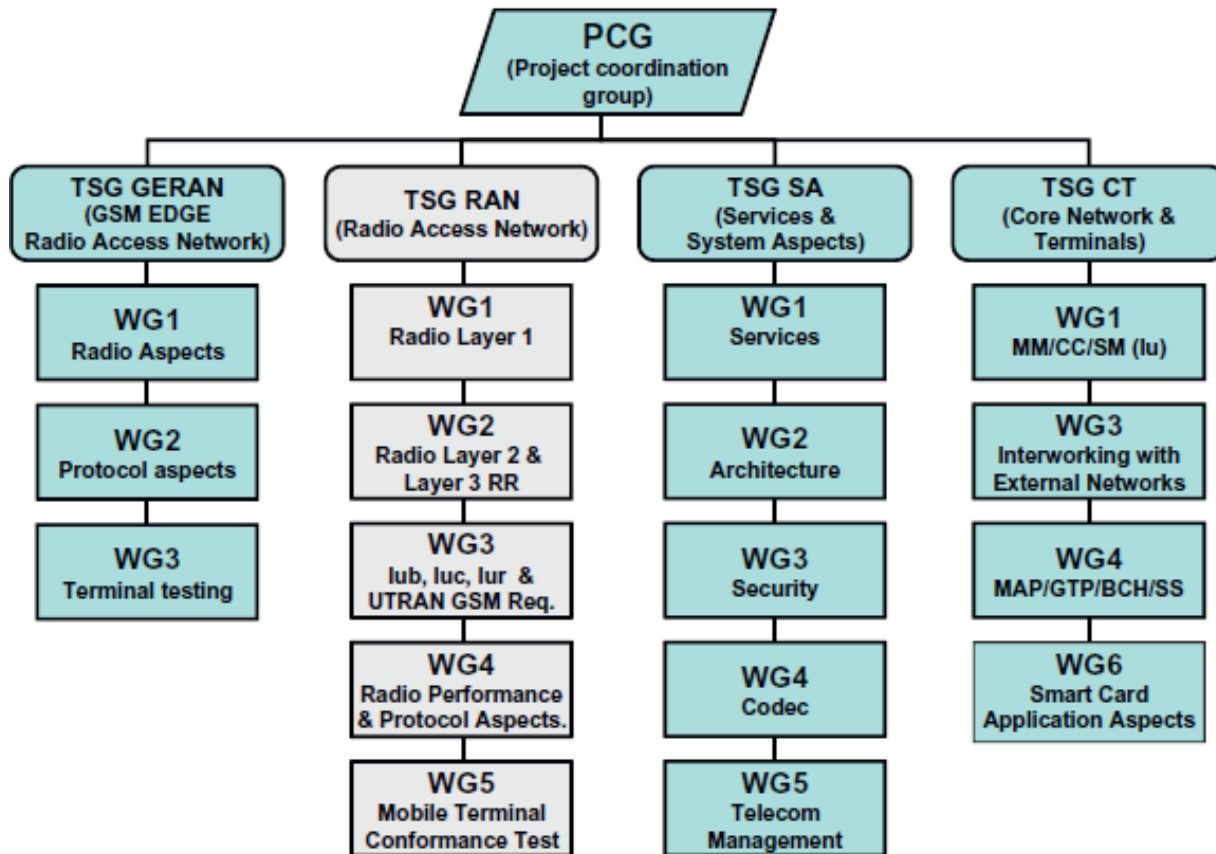


Figure C - 1. 3GPP organization structure.

3GPP working groups included the following initial priorities:

- Common global radio electric spectrum: 1.920-1.980 MHz and 2.110-2.170 MHz.
- Wide range of new services.
- Focus in data (e.g. Internet) and multimedia oriented.



- Data transfer rate up to 2 Mbps.
- Seamless global roaming.
- Enhanced performance and security.
- Support to a wider variety of terminals.
- Exhaustive use of Intelligent Networks.

This annex will focus in 3GPP (UMTS) releases for third generation mobile communications. 3GPP2 work is out of the scope of this work.

### C.1.1 3GPP UMTS R99 and R4 main characteristics

Next are detailed the main characteristics of UMTS according to 3GPP first releases, i.e. from UMTS R99 to R4:

- New radio access network: UTRAN (UMTS Radio Access Network) using WCDMA in the air interface. As GSM and WCDMA user equipment are incompatible, thus a couple of network elements are introduced for backward compatibility between UMTS and GSM network subsystems:
  - RNC (Radio Network Controller): replaces GSM/GERAN's BSC.
  - NB (Node B): replaces GSM/GERAN's BTS.
- 5 MHz spectrum (24 times the one used for GSM).
- ATM (Asynchronous Transfer Mode) is initially adopted as transport technology between UTRAN nodes (later is replaced by more efficient MPLS -Multi Protocol Label Switching-).
- CAMEL: ability to transfer information across networks and capacity to involving in all transactions between them.
- CS CN elements able to handle 2G and 3G subscribers:
  - Update needed for MSC/VLR, HLR/AuC and EIR.
  - SGSN.
  - Mobility Management (MM) divided between RNC and SGSN.
- Services:
  - Initially 3G offers the same services as 2G.
  - Services are shifted to the PS CN.
- Trends:

- Separation of concerns by splitting connections for signaling and services/data/media (control and user planes).
- Shift to all IP-based network (adoption of SIGTRAN or SS7 over IP).
- Network provided multimedia services: IP Multimedia Subsystem (IMS).

#### C.1.1.1.1 Wideband Code Division Multiple Access (WCDMA)

UMTS introduces a sensitive enhancement in transceiving information speed/data rate through substantial adjustments in access and signal modulation technologies, namely:

- Traditional GSM' TDMA/FDD (Time Division Multiple Access / Frequency Division Duplex) evolves to **WCDMA** (Wideband Code Division Multiple Access). WCDMA introduces then a paradigm shift from TDMA/FDMA as all users receive the signal under a single carrier frequency, discerning them by applying the corresponding orthogonal code. As these codes applied for each signal are orthogonal between each other, where a high auto-correlation and low cross-correlation exists among the distinct signals. In other words, all signals are cancelled or filtered as white Gaussian noise except the one assigned with the same code at the receiver, which in fact is amplified.
- **Spread Spectrum.** Bits to be transmitted are transformed by orthogonal codes into «chips», i.e. bits of shorter wavelength. Hence, chip bandwidth is greater than the information bandwidth implicitly transmitted (which is recovered in the receptor by applying the corresponding negotiated orthogonal code).
- **Rake Receiver.** Another relevant aspect introduced in the UMTS UE is the «Rake Receiver», which encompasses multiple input antennas for cancelling the interference produced by multipath signal reception mainly due to signal reflection, but also scattering, diffraction or refraction). Received multipath signals are copies of each other with different amplitudes, phases, delays, polarity and angle of arrival. If the code sequence has an ideal auto correlation, then it will be zero out of the  $[-T_c/2, T_c/2]$  interval, where  $T_c$  is the chip time interval. This indicates that if the expected signal and delayed versions of it are

received in time intervals longer than  $T_c$ , modulation will deal with the delayed version as a different signal. The «Rake Receiver» is composed of multiple correlators synchronized with most relevant replicas arrival times according to channel permanent analysis, thus counteracting unsynchronized interference caused by multipaths. For replicas arriving with delays greater than  $T_c$ , i.e.  $0.26 \mu\text{s}$ , the WCDMA receiver may distinguish and combine them coherently for producing temporal signal diversity. By correlating replicas by the spreading spectrum orthogonal code, synchronized with the arrival instant of each replica, shrinking of the replicas is obtained. The sum of all these operations for the first three signal branches or «fingers» sync with bit or frame interval, derives in multipath interference cancellation.

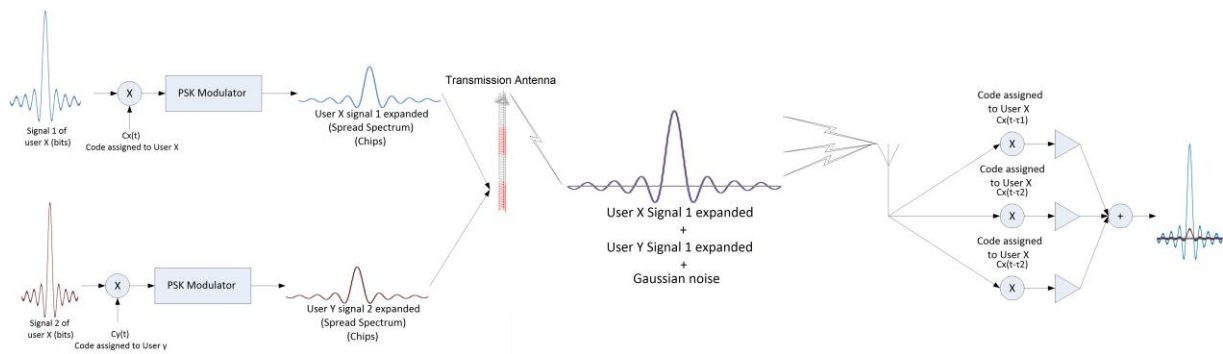


Figure C - 2. WCDMA Spread Spectrum transmission and reception with Rake Receiver.

- **Soft Handoff.** This process happens when the UE finds itself in the overlapping area of adjacent cells. Communication between NBs and the UE are established through different channels from the adjacent cells. Signals on both channels are received by the UE in order to generating the corresponding orthogonal code for each signal. Then, a new connection is established before the ongoing communication is cut off and the handoff is completed when moving from one cell to the other. Hence, the brief interruption perceived in previous RAN accesses no longer exists in WCDMA.
- **Power control and macro-diversity.** WCDMA makes terminal's power control necessary so as to cancelling the interference caused by the «near-far effect», which derives from the of reception of signals with different power at the base station or NB in function of the distance between them and the mobile station

(which beyond UMTS release is named as UE for «User Equipment»). Hence, UE transmission power control is carried out so that same power is received from all of them at the NB. In other words, most distant UEs transmit at higher power than those closer to the NBs. Likewise, this fact could potentially cause interference among those distant UEs between each other, thus another concept is introduced named «macro-diversity», by which an UE near to the cell limit might be linked to multiple cells simultaneously. Then, the downlink signal transmission (NB→UE) is transmitted from all NB the UE is attached to. Equally, in the uplink transmission path (UE→NB), the signal is received and processes by all involved NBs. Both the UE and the UTRAN combine the received signal in a way to cancel introduced errors by multipaths. This redundancy also allows reducing the UE's transmission power and thus, reduce interference.

- Modulation technique adopted initially is QPSK (Quad Phase Shift Keying). QPSK uses four orthogonal sinusoidal signals for coding each consecutive pair of symbols or bauds (bits/chips). Later, 8PSK is adopted, where three bits of information are transmitted per each baud.

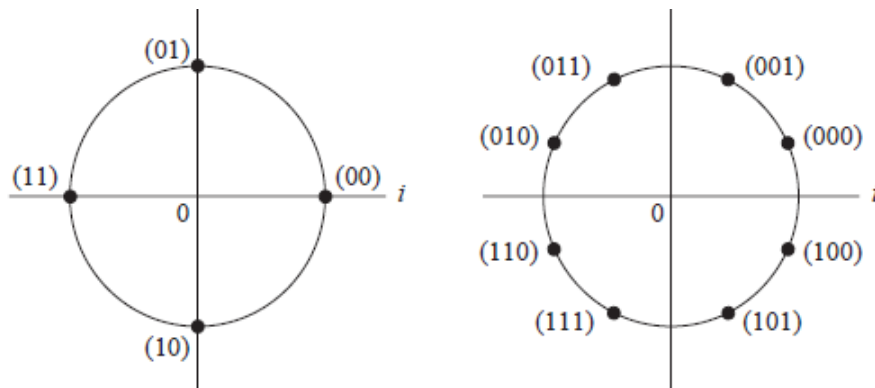


Figure C - 3. QPSK and 8PSK modulation scheme constellations.

### C.1.2 UMTS Releases 6 Network Architecture

Throughout this section, release 6 of 3GPP for UMTS network architecture shall be briefly detailed. Some of the components described were already introduced in release 4. However, release 6 is particularly important as the IMS is introduced. Some of these components were introduced in earlier releases as explained further.

### C.1.2.1 UTRAN

Briefly, the UTRAN establishes the connections between the US and the rest of the network. Is composed by the following components:

- Radio Network Controller (RNC). Its basic functions are controlling radio resources, i.e. frequency assignment, power level control, orthogonal code management.
- Node B (NB). It provides service access to a specific cell and is controlled by one RNC.

### C.1.2.2 UMTS Circuit-Switched Core Network

The UMTS CS CN maintains general aspects of GSM NSS. It comprises a Network enabled to providing voice and data services with separation of concerns between the control and data plane.

3GPP R4 introduces connection split for control and services in the CS CN domain. GSM NSS nodes also need to escort this evolution. The MSC encompasses connection capabilities as well as connection control, although not necessarily are accomplished together. Beyond 3GPP R4 specs, the way these capabilities must be split is two different nodes is defined. These nodes are:

- **MSCS (MSC Server)**: responsible of mobility management and mobile originated/terminated calls switching in the CS CN domain. Mobile subscribers being provided service by the MSCS have their updated CAMEL subscription, service and location information held at the MSCS' associated VLR. The GMSC Server is to a GMSC as an MSCS is to an MSC.

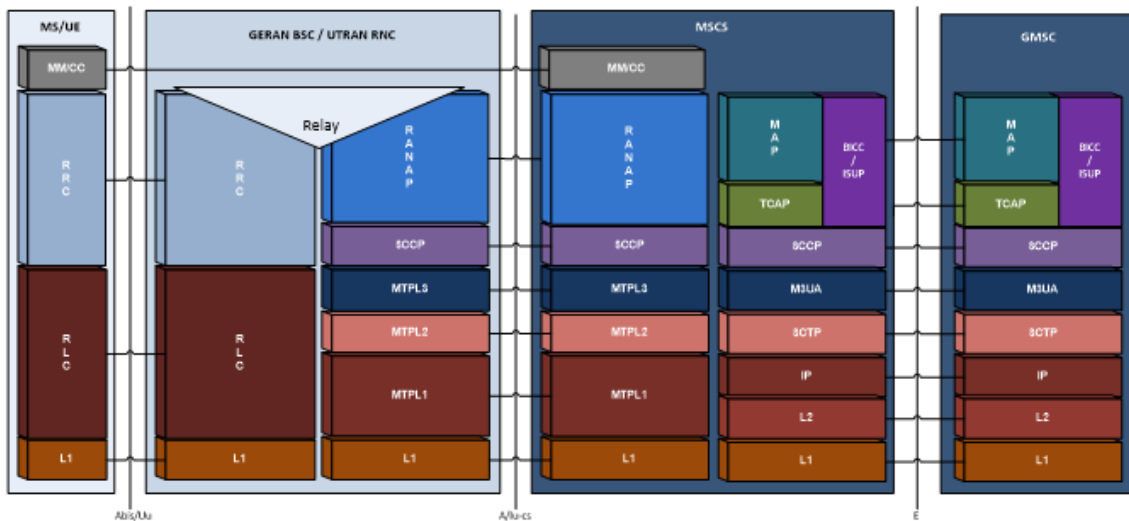


Figure C - 4. MSCS control plane user-network and network-network signaling.

At the user's plane, the MSCS controls the parts of the call state that pertain to connection control for media channels in a CS-MGW. A connection represents an association between an input and output point at the CS-MGW. The input point could correspond to a voice circuit termination (A or luCS according to GERAN or UTRAN respectively). The output point could be assimilated by an RTP/UDP/IP or AAL2/ATM port. MSCS controls the CS-MGW via a ITU-T H.248/MEGACO protocol interface.

At the control plane, the MSCS terminates user-network signaling (BSSAP or RANAP), turning it into relevant network-network signaling (MAP, ISUP or BICC, CAP).

- CS-MGW (Circuit Switched Multimedia Gateway).** The CS-MGW is the PSTN/PLMN transport termination point for a defined network and interfaces UTRAN RNC or GERAN's BSC with the core network, receiving media traffic (audio/video) and routes it to an IP network over an ATM/MPLS backbone. It interacts with the MSCS and the GMSCS for resource control, as well as the IMS MGCF (Media Gateway Control Function) through ITU-T H.248/MEGACO.

A CS-MGW may also terminate bearer channels from a circuit switched network and media streams from a packet network (e.g., RTP streams in an IP network). As the entity interfacing the access and the core network, the CS-

MGW operates the requested media conversion it contains (e.g. the TRAU), the bearer control and the payload processing (e.g. codec, echo canceller, conference bridge). It supports the different lu options for CS services (AAL2/ATM or RTP/UDP/IP based).

The CS-MGW bearer control and payload processing capabilities also need to support mobile specific functions such as SRNS relocation/handover and anchoring. ITU-T H.248/MEGACO standard mechanisms are applied to enable this.

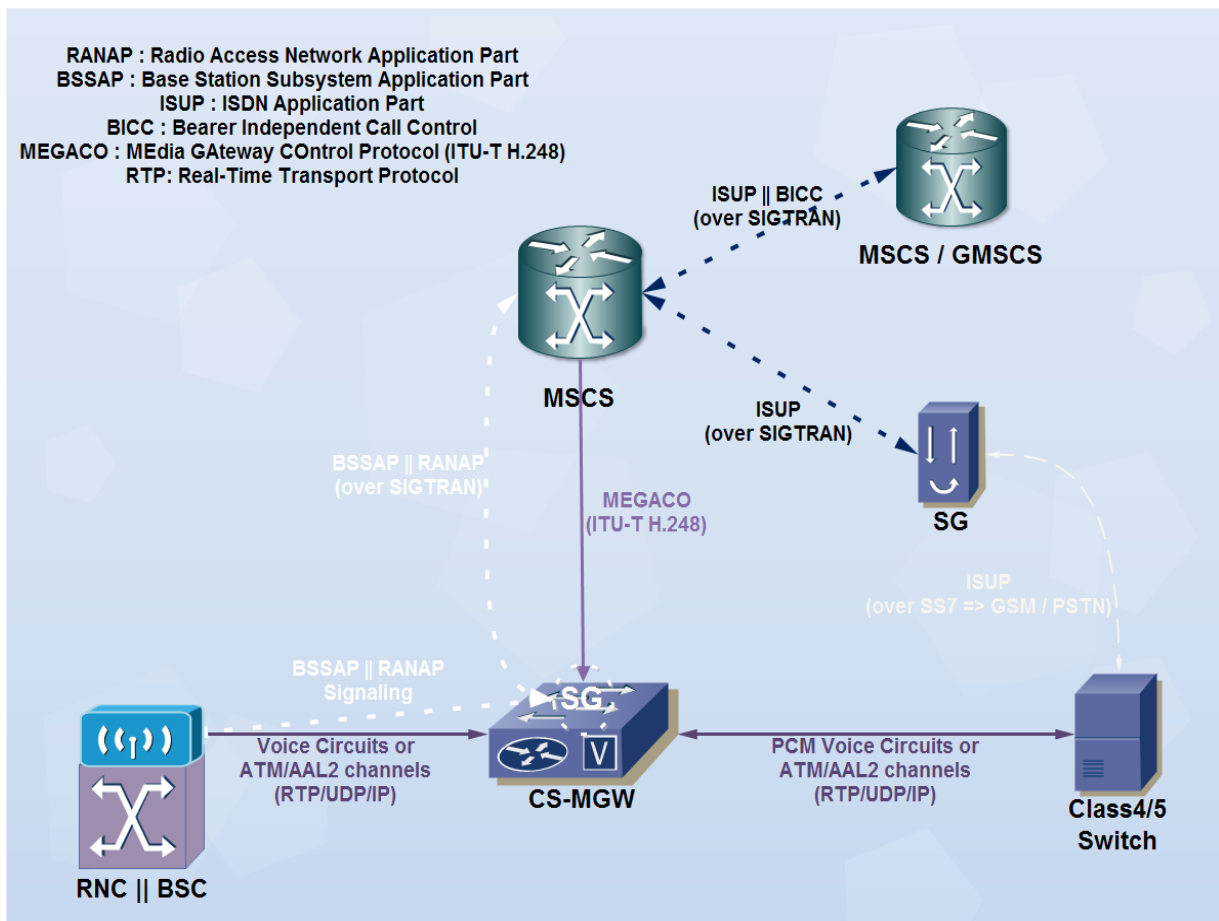


Figure C - 5. MSCS – CS-MGW signaling.

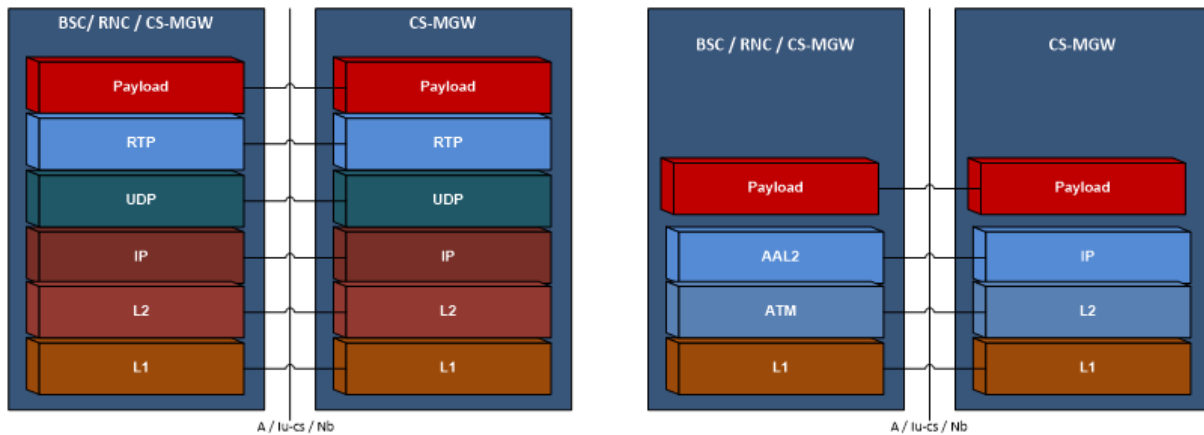


Figure C - 6. User plane user-network signaling at the CS-MGW either RTP/UDP/IP or AAL2/ATM based.

### C.1.2.3 IP Multimedia Subsystem (IMS)

Release 6 of 3GPP defines the IMS for the UMTS. Stage 2 is now defined under 3GPP TS 23.228 specification [33]. This section shall briefly describe its main components, protocols, interfaces and interworking with the UMTS, as well as Policy and Charging Control (PCC).

#### C.1.2.3.1 IMS Components

Following are briefly described the main components of the IMS.

- **HSS (Home Subscriber Server).** The HSS constitutes a database containing all subscriber's information needed for managing multimedia sessions. It is responsible of holding the following subscriber related information (accessible through Diameter interfaces):
  - Subscriber's identity, number and address.
  - Subscriber's security information, i.e. access network control information for authentication and authorization.
  - Subscriber's location information at inter-system level: the HSS supports user registration and stores inter-system location information.
  - Subscriber's profile information.



- The HSS also generates subscriber's security information for mutual authentication, data integrity and cyphering. Based on this information, the HSS is responsible for call control as well as session management entities of different domains and subsystems.

The HSS also has IP Multimedia capabilities for provisioning of IMS control functions such as the CSCF (Call Session Control Function). HSS and CSCF are interfaced via Diameter [31].

HLR/AuC functionalities required by either GPRS PS CN or LTE EPC are hold by the HSS.

HLR/AuC functionalities required by the CS CN are also held by the HSS if access to CS CN subscribers is requested, e.g. for supporting roaming to CS CN legacy domain such as GSM NSS or UMTS CS CN.

- **SLF (Subscriber Location Function).** It comprises a database for mapping subscribers with existing HSSs. Hence, it only makes sense if more than one HSS is present in the network.

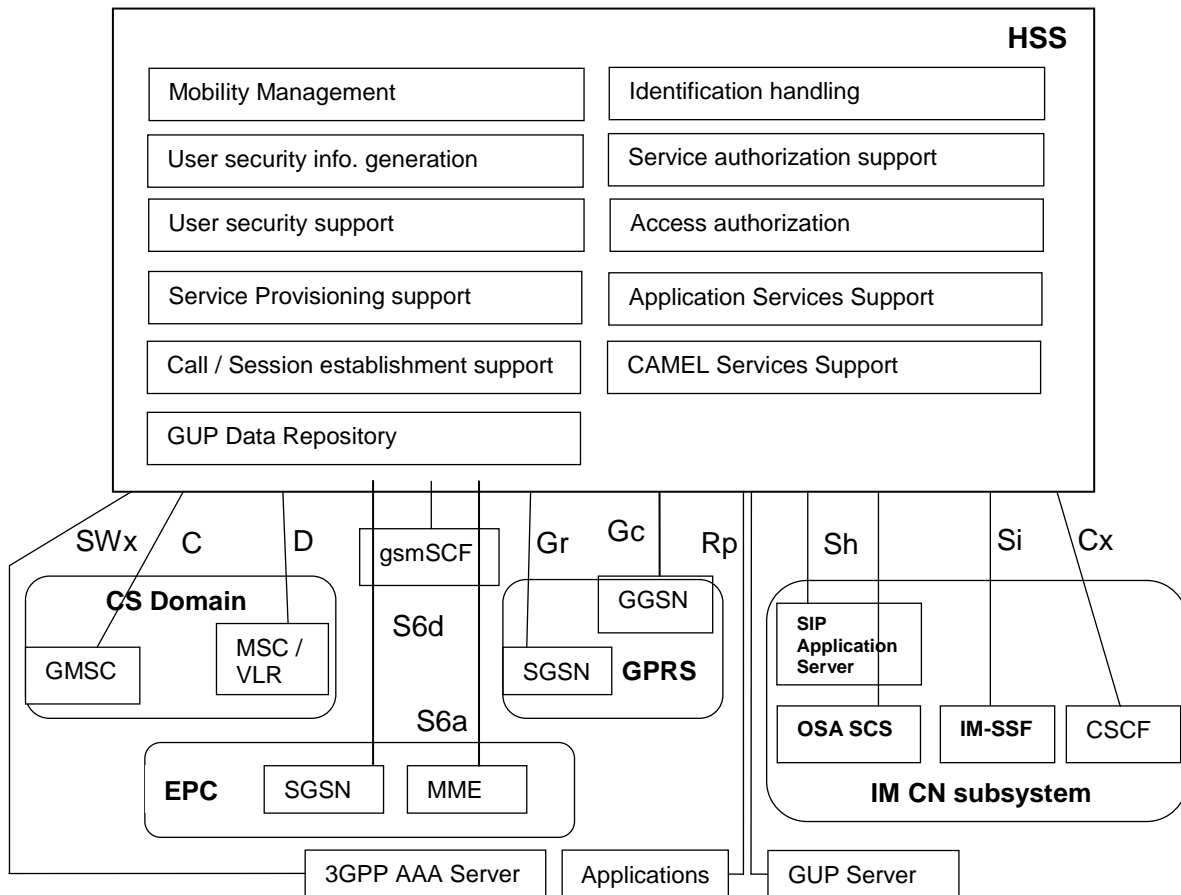


Figure C - 7. HSS logic functions and interfaces with entities of the CS and PS CNs as for 3GPP TS 23.002.

- **P-CSCF (Proxy - Call Session Control Function).** When establishing an interface with the GGSN or PDN-GW (LTE EPC), it constitutes the first point of contact in the control plane encompassing the network node through which all signaling traverses between the UE and the IMS.

The P-CSCF acts as an AF (Application Function) offering resource control for an IP bearer or charging flow control to demanding applications. It is able to communicate with the PCRF (Policy and Charging Rules Function) for transferring quality of service (QoS) and/or charging related dynamic information.

The P-CSCF includes functions like the one following:

- SIP register request retransmission as received from the UE towards a determined entry point by using the origin domain name, as provided by the UE.
  - Retransmission of incoming SIP messages from the UE towards the appropriate SIP server (e.g. S-CSCF) whose name has been received by the P-CSCF as part of the registration procedure.
  - Guarantee that SIP messages received from the UE towards the appropriate SIP server (e.g. S-CSCF) contain correct and updated information according to the network access type used currently by the UE, whenever the information is available from the access network.
  - Maintain a secure association with each UE.
  - Data integrity assurance/protection through IPsec associations.
  - Verification of correct SIP message format.
  - Detection and management of an emergency session establishment request.
  - User authentication in every IMS node, so that these do not have to re-authenticate during the session.
  - Compression/Decompression of SIP messages.
  - Resources and QoS authorization in the user plane through the PDF (Policy Decision Function).
  - CDR (Call Detail Records) generation.
  - Detection and management at IMS session establishment request or termination.
- **I-CSCF (Interrogating - Call Session Control Function)**. Constitutes a point of contact in the operator's network for all connections destined to a subscriber of such MNO or to a user currently roaming within it. It works as a proxy located at the frontier of an administrative domain. When a SIP server follows procedures for finding the next SIP hop for a particular message, the SIP server obtains the I-CSCF address of the destination domain. Functions carried out by an I-CSCF include the following:
    - Registration.
      - Assignment of an S-CSCF to a user performing a SIP registration.
    - Information flow functions session and non-session related.

- Routing a SIP request received from another network towards the S-CSCF.
- E.164 address translation included in every request containing a SIP URI with the parameter «user=phone» to the format «Tel:URI» of IETF RFC 3966, previous to the HSS location query. In case the user does not exist and if being set by the operator's policy, the I-CSCF may invoke the transit functionality that translates the E.164 address contained in the request from «Tel:URI» to a routable SIP URI.
- Retrieve the S-CSCF address from the HSS through Diameter.
- Retransmission the SIP request or response to the S-CSCF determined by the HSS.
- Traffic routing functions.
  - Based on a query to the HSS, if the I-CSCF determines that the session destination is not within the IMS, it may forward the request or answer with a release cause to the originating party.
- Charging or resource use related functions.
  - CDR (Call Detail Records) generation.
- **S-CSCF (Serving - Call Session Control Function).** Central node in the control plane in the IMS, therefore, it carries out all session control services for the UE. Additional to the SIP server functionality, the S-CSCF also acts as a SIP Register, meaning that it maintains a bond between the user location and the registered IP address (also known as Public User Identity -contained in the IMS SIM or ISIM-).

The S-CSCF implements a Diameter interface with the HSS for authentication and retrieval of user profile vectors, as well as establishing S-CSCF identity in the HSS during the registration procedure.

The S-CSCF also applies policies for preventing users to carrying out unauthorized activities.

It may apply traffic routing functions within specific IMS scenarios, E.164 address translation to a globally routable SIP URI (in case of translation failure,

the request might be transmitted to the BGCF so as to allowing routing to the PSTN and in case of a successful translation, the requested URI is updated and the request routed based on the obtained SIP URI).

The S-CSCF may also provide termination points with information related to service events (e.g. play announcements together with additional resource assignment, charging notification, etc.). It may also generate CDR (Call Detail Records).

- **SIP-AS (SIP Application Server)**. Encompasses a service container and IP multimedia services executor based on SIP protocol (ISC -IMS Service Control- interface with the S-CSCF).
- **OSA-SCS (Open Service Access – Service Capability Server)**. Acts as SIP-AS towards the IMS (establishing an ICS-SIP with the S-CSCF) and an OSA-AS interface and OSA API as for 3GPP TS 29.228.
- **IMS-SSF (IP Multimedia Service Switching Function)**. It allows IMS session control by a gsmSCF. The IMS-SSF acts as a SIP-AS with the IMS (SIP interface with S-CSCF) and as a SSF with the CS CN by establishing a CAP interface with the corresponding gsmSCF.
- **PSTN Gateway**. It comprises the following nodes:
  - **SGW (Signaling Gateway)**. Node responsible for translating ISUP or BICC over TDM/MTP to ISUP or BICC over SIGTRAN (SCTP/IP).
  - **MGCF (Media Gateway Controller Function)**. Also known as «Softswitch», it's the central node of the PSTN Gateway. It implements a state machine that performs protocol conversion and maps SIP either towards ISUP or BICC over IP. Besides, it controls MGW resources via a ITU-T H.248/MEGACO interface.
  - **MGW (Media Gateway)**. It establishes an interface in the media/user plane with the PSTN or CS CN. On one side (IMS), it is capable of transmitting and receiving multimedia data via RTP, meanwhile on the other side (PSTN or CS CN) it uses PCM/TDM timeslots information for connecting with the

Circuit-Switched Core Network. Additionally, it may perform transcoding when the IMS terminal does not support the CS CN used codec.

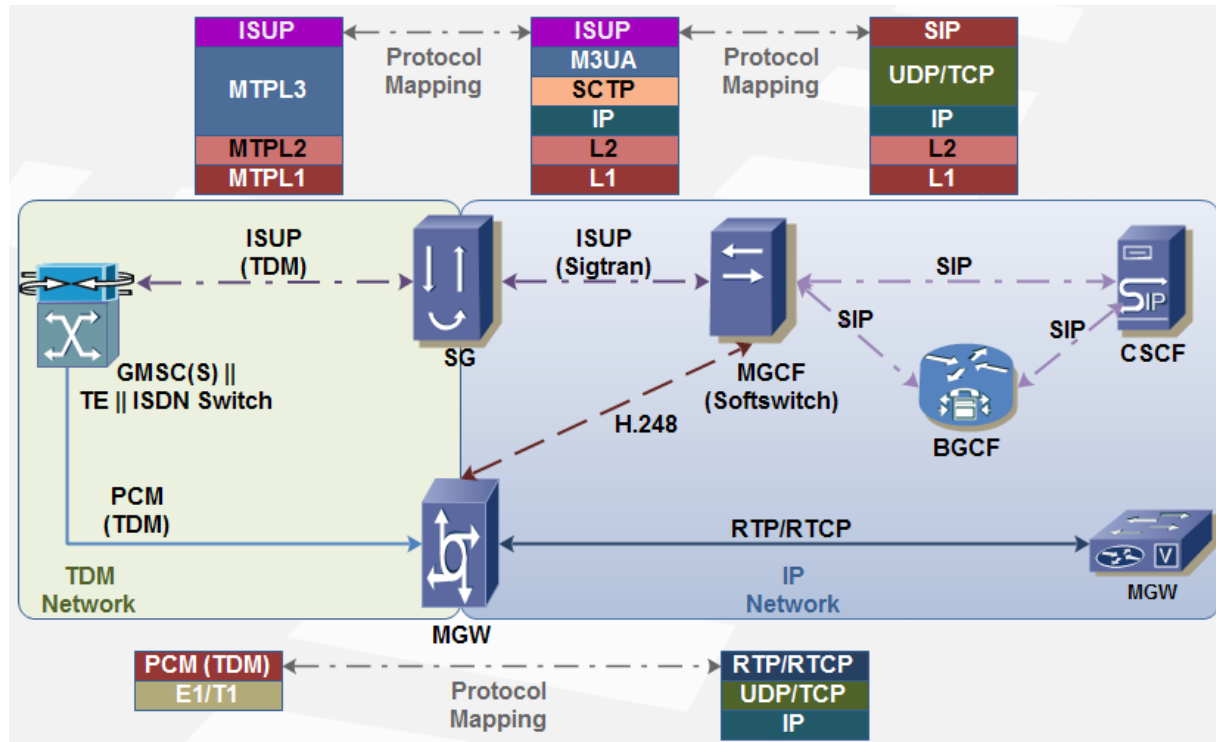


Figure C - 8. PSTN Gateway protocol mapping.

- **BGCF (Breakout Gateway Control Function).** It essentially constitutes a SIP server including routing ability based on telephone directory numbers. It is used when the IMS destined a call towards a user of the CS CN (PSTN or PLMN). The main functionality of the BGCF is then decomposed into one of the following:
  - Select the appropriate network where the interaction with the CS CN must happen.
  - Select the PSTN/CS Gateway if the interaction will happen within the same network where the BGCF is located.

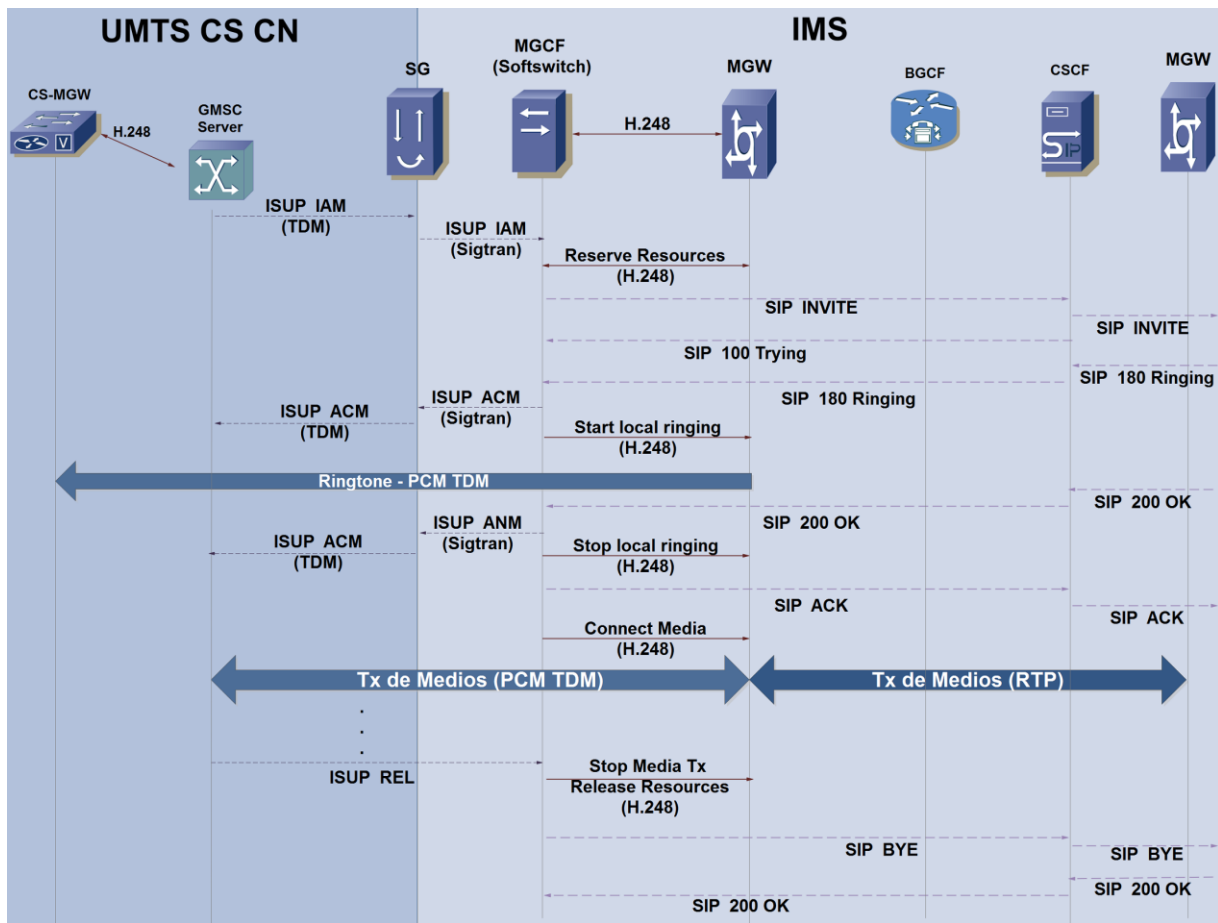


Figure C - 9. UMTS-IMS call flow.

- PCRF (Policy and Charging Rules Function).** Point in the network where authorization and charging policies are applied. To execute the decisions, the PCRF receives information from AF (Application Functions, such as P-CSCF or an AS) and the SPR (Subscription Profile Repository). An AF provides the PCRF with information retrieved from the session control plane (especially from request/response message exchanges from an SDP) over the R<sub>x</sub> Diameter based interface.
- SPR (Subscription Profile Repository).** Provides the PCRF with QoS information related to the subscriber's subscription information through the S<sub>p</sub> interface (via Diameter or LDAP).

- PCEF (Policy and Charging Enforcement Function).** Decisions executed by the PCRF are forced by the PCEF, which constitutes a logic function inside a Gateway (GGSN or PDN-GW). The PCRF communicates with the PCEF through the G<sub>x</sub> Diameter based interface.

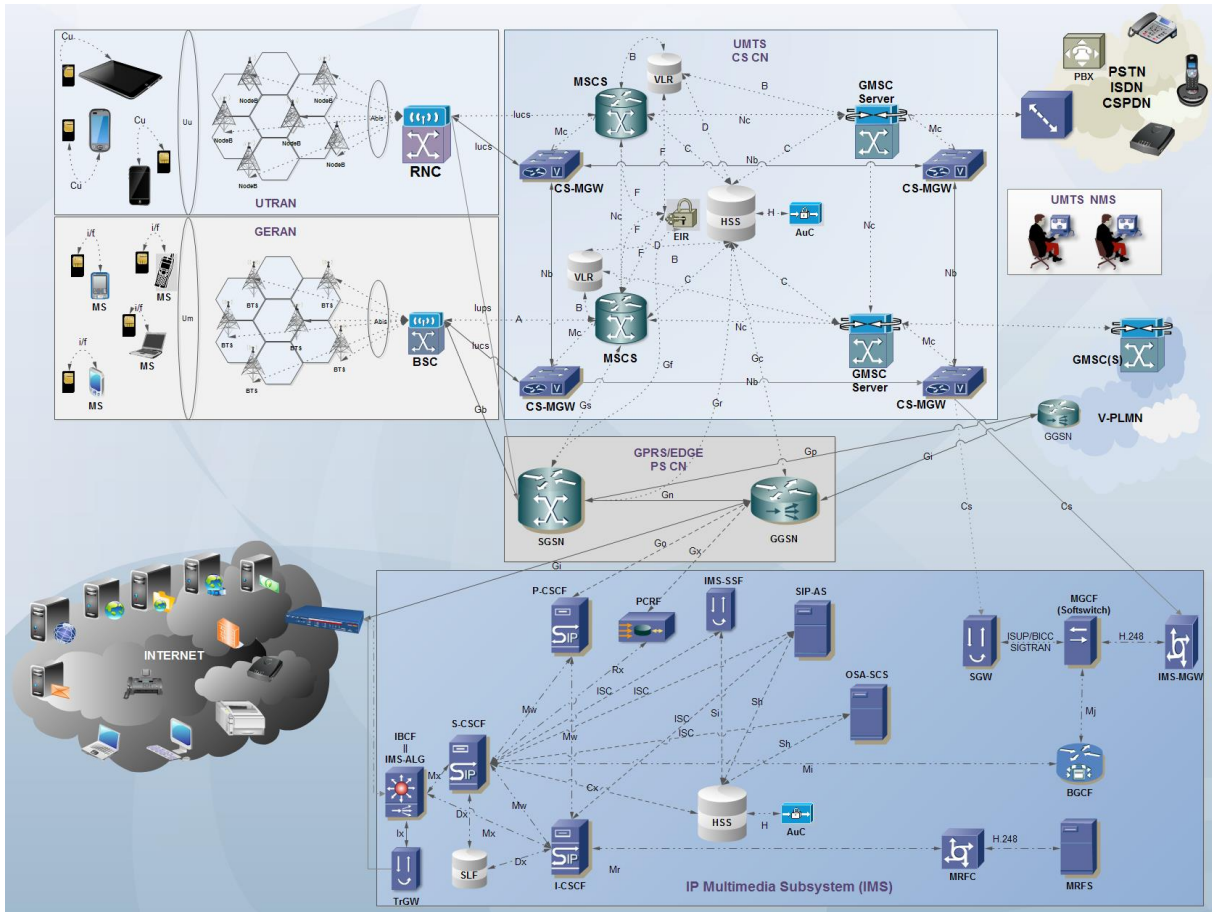


Figure C - 10. GSM/GPRS/UMTS/IMS internetworking.

### C.1.2.3.2 IMS Communication Protocols

Following are briefly introduced the main communication protocols used in the IMS, namely:

- SIP (Session Initiation Protocol):** used for IP multimedia session control.



- Diameter: used for subscriber status and location queries, and AAA (Authentication, Authorization and Accounting).
- ITU-T H.248: used by signaling and control nodes in the user plane (e.g. Media Gateway Controller Function – Media Gateway).
- RTP/RTCP: used for real time transmission of media (audio/video).

## C.2 Brief Introduction to NGN

NGN paradigm rises from the understanding of fixed and mobile intelligent legacy networks limitations for the collaboration with third parties in services creation and decoupling from network infrastructure, as well as the need of a shorter time-to-market.

NGN enables CSPs to share resources and infrastructures, facilitate interoperability between networks, simplify and unify OA&M and service offer and therefore, enable a fast and cost-effective creation of new and customized ubiquitous wideband services. This allows third parties taking advantage of the telecommunication's capabilities within their own environments and at the user's side, NGN allows access to services that were excluded in legacy networks due to signaling high latency, poor performance, etc.

Out of these concepts, final users can then enjoy customized mobile wideband services at any time and everywhere, as well as counting on service flexibility and variety they already enjoy in the Internet.

According to ITU-T Y-2012, a Next Generation Network is defined as a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users. The NGN is characterized by the following fundamental aspects:

- Packet-based transfer.

- Separation of control functions among bearer capabilities, call/session, and application/service.
- Decoupling of service provision from transport, and provision of open interfaces.
- Support for a wide range of services, applications and mechanisms based on service building blocks (including real time/streaming/non-real time services and multi-media).
- Broadband capabilities with end-to-end QoS and transparency.
- Interworking with legacy networks via open interfaces.
- Generalized mobility.
- Unfettered access by users to different service providers.
- A variety of identification schemes which can be resolved to IP addresses for the purposes of routing in IP networks.
- Unified service characteristics for the same service as perceived by the user.
- Converged services between Fixed and Mobile networks.
- Independence of service-related functions from underlying transport technologies.
- Support of multiple last mile technologies.
- Compliant with all Regulatory requirements, for example concerning emergency communications and security/privacy, etc.

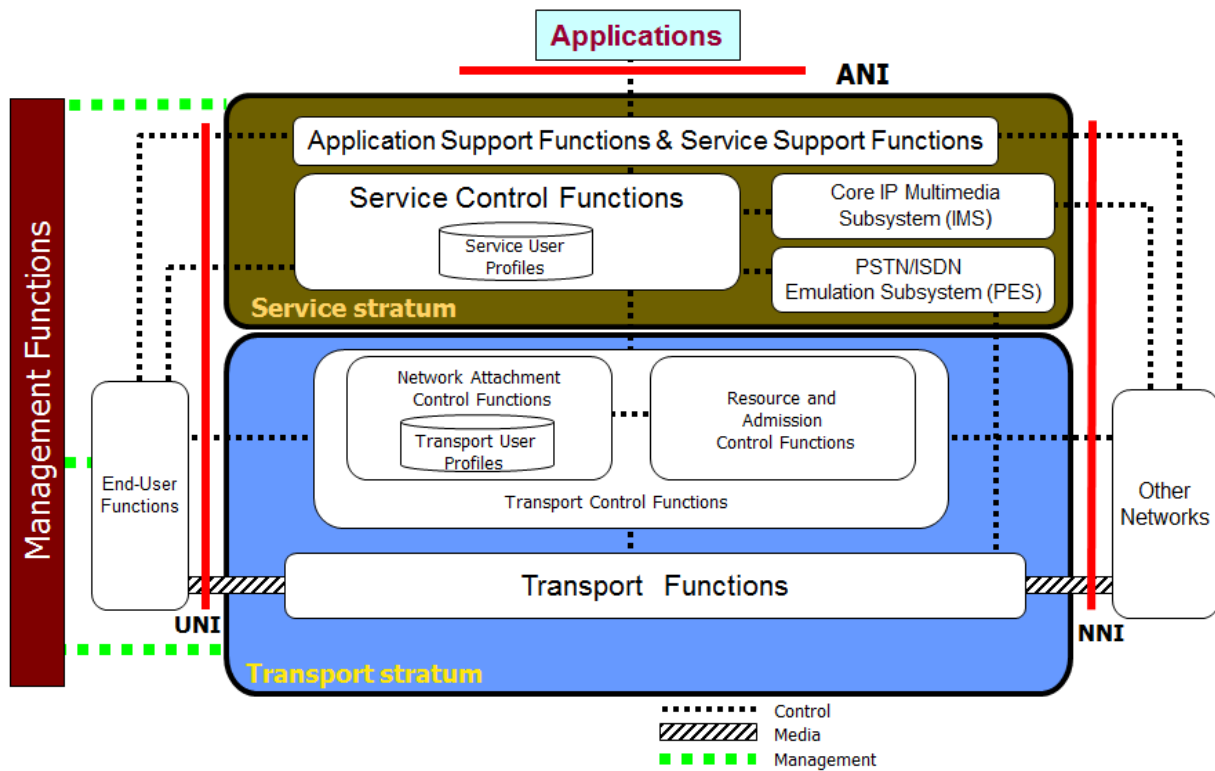


Figure E - 1. NGN Architecture view according to ITU-T Y-1202.

### C.2.1 NGN Layers

According to [146], NGN layers are as following:

- **Access Layer:** Combination of all access technologies such as PSTN, ISDN, GSM/GPRS/UMTS/LTE, HFC, LMDS (Local Multipoint Distribution Service), ADSL, etc.
- **Transport Layer:** IP Trunking network and transport technologies (currently based on MPLS).
- **Control Layer:** Call control management. It comprises the nodes in charge of signaling (SG, Signaling Gateway) and call processing (MGC, Media Gateway Controller, also known as «Softswitch»).

- **Service Layer:** Responsible for Operations/Business Support Systems (OSS/BSS). Enhanced services are provided to the users helped by an Application Servers, which may introduce any service at any time, without control modification, its transport or access technology.
- **Management Layer:** It covers all the layers, integrating every management equipment.

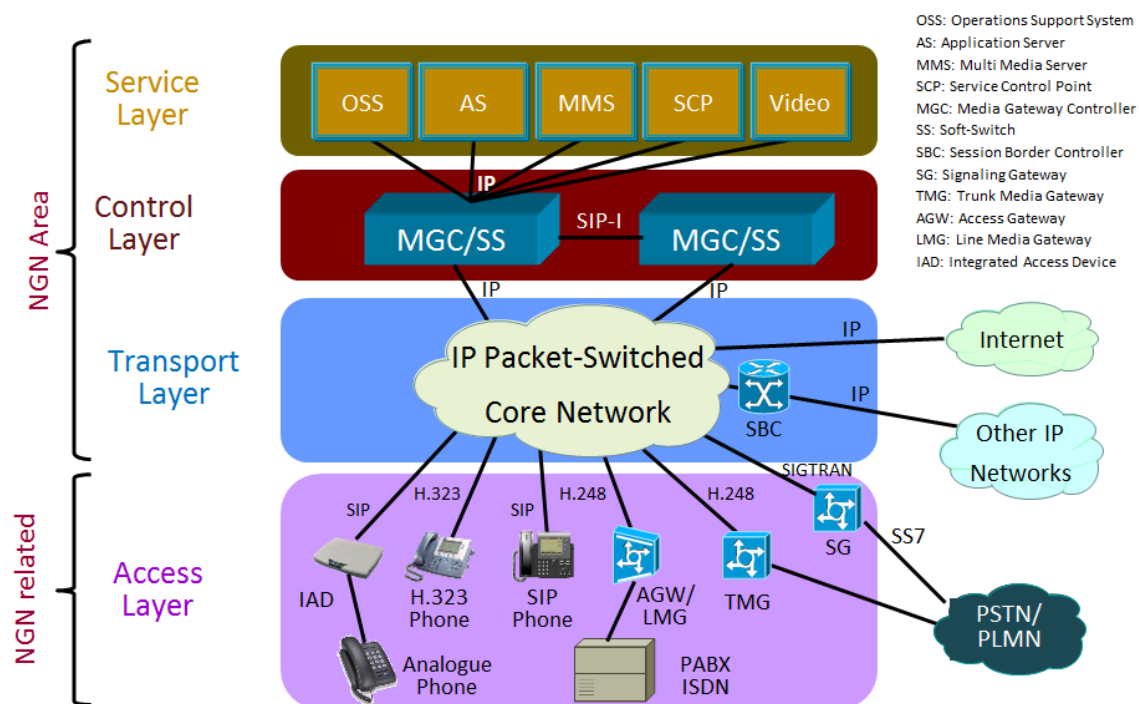


Figure E - 2. NGN layer model according to [145].

### C.2.1.1 Session Border Controller (SBC)

SBC also known as IBCF (Interconnection Border Control Function) is a new functional entity introduced by NGN, which, as with most changes to IMS, has been also adopted by 3GPP IMS. The SBC acts as a separation between two different domains. Typically, it is the first SIP node that gets a SIP request from an external domain, replacing the I-CSCF as the original first entry point. The IBCF can also be the last node in the signaling path prior to the forwarding of the SIP request to an

external domain. The main functionality of the IBCF is to screen the signaling, and obfuscate those SIP headers that the operator considers dangerous to expose externally. The SBC may also integrate an Interworking Function (IWF) which can provide interworking with other signaling protocols, such as H.323.

SBC are then specialized devices that operate as an interface between IP networks with SIP and/or H.323, comprising an NGN evolution of first IP Gateways providing services such as NAT (Network Address Translation), firewall and billing at the edge of the network. Then, SBC are widely used in VoIP networks originally designed to operate as NAT in subnets within an IP service network or as network elements at the edge of a VoIP network for interaction with the PSTN.

Among SBC basic functions, the following are highlighted:

- NAT for signaling or media traffic at the edge of networks or subnetworks. Hence, they hide network topologies to both sides, preventing acknowledge of network entities or how calls are routed.
- SIP, H.323, etc. messages control, eliminating errors which might cause inconvenience among network entities, and by adapting SIP headers to public and private IP addresses.
- SBCs may operate as SIP ↔ H.323 translators, resolving signaling and media conveyance. They may adapt media codecs.
- SBCs may operate as firewalls or force one to its duty.
- SBCs allow media and signaling to go through a firewall without modification. A mechanism is the introduction of pinholes in the firewall for SIP or H.323 signaling transport and media advance, along with the «keep alive» mechanism, non-existent in H.323.
- SBCs allow security measures such as call admission and mitigation of DOS (Denial of Service) / DDOS (Distributed Denial of Service) attacks.
- Support for CALEA (Communications Assistance for Law Enforcement Act), for lawful interception.
- Billing support, allowing the whole traffic control exchanged between operators, quota fulfilment, prepaid traffic control, origin or destination routing restriction control, cost restrictions. It generates CDRs for accounting conciliation between operators.

- QoS policies support, by controlling bandwidth assigned to calls and reservation for emergency calls.

NAT functionality, extended to NATP (NAT Port Translation), was created in IETF RFC 1631 for allowing the integration of IPv4 subnets using private IP addresses, which are repeated among private networks. Hence, for avoiding problems in massive use of private IP addresses, IPv4 public routers are banned to routing packets holding private addresses (of CIDR ranges 10.0.0.0/24, 172.16.0.0/20 and 192/168.0.0/16), they must immediately discard them. The usage of NAT implies the operation of a double input table, public and private with IP address, protocol and port at each side. A NAT operates as a proxy for other IP networks, as it only offers an IP address while it internally maps distinct private IP addresses among different ports.

NAT/NATP present problems in SIP or H.323 networks with incoming calls, as outgoing calls do not have troubles with IP translation. SIP messages transport IP addresses at application level over IP and NAT layers. If an incoming message to a SIP network includes an IP address in the response, it cannot be resolved through NAT and thus will not reach the destination user agent. For example, a «100 Trying» response message to an INVITE request (SIP messages will be explained further in Annex E) including the header field «Contact» with a private IP (e.g. Bob@10.0.0.125), it cannot reach the proxy server of «Bob» SIP network and therefore, the call will not be established. SBC solve this kind of problems by operating at SIP application layer, as they are conscious of the SIP messages body content. When an INVITE with the header field «Contact: Bob@10.0.0.125» arrives to an SBC, it modifies the header field for the response to the INVITE request by setting a different SIP URI in the «Contact» header field and an association between both SIP URIs in a table. When a «100 Trying» or «200 OK» response arrives to the remote endpoint user agent, the SBC restores the «Contact» header field to the original SIP network private IP and so the SIP session establishment may proceed.

## Annex D

### D Long Term Evolution (LTE)

#### D.1 Introduction to LTE

LTE is UMTS' evolution towards 4<sup>th</sup> generation of mobile communications. The 3GPP started working on LTE by 2004 and standardization begun by Release 8 in 2008. It has been conceded as 4G albeit it does not fit ITU-R aims defined for Advanced IMT, namely:

- Peak data rate of up to 1 Gbps.
- Worldwide functionality and roaming among different type of networks.
- Services compatibility.
- Internetworking with other radio access network systems (e.g. WiMAX).

Main characteristics of LTE first releases are described next:

- Variable bandwidth per MNO (1.4, 3, 5, 10, 15 y 20 MHz) for cost effectiveness and allow use of assigned bands. Support of up to 200 active users per 5 MHz LTE cell.
- Native support architecture for MIMO (Multiple Input Multiple Output) and very high speed:
  - 100/75 Mbps Downlink/Uplink (20 MHz bandwidth).
  - Spectral efficiency of up to 15/7,5 bps/Hz in Downlink/Uplink.
- Evolved UTRAN (E-UTRAN) architecture:
  - IP/MPLS based.

- Reuses concepts such as logical, transport and physical channels and MAC, RLC, RRM protocol stack layers.
  - Node B and RNC integrated in a unique entity: eNodeB (eNB).
  - Cells of up to 100 Km.
- OFDMA (Orthogonal Frequency Division Multiple Access) introduced in the downlink. By using Direct/Inverse Fourier Transforms (DFT/IFT), OFDM uses the power of two orthogonal sub-carriers, each one modulated in QPSK, 16QAM or 64 QAM. Orthogonality is passed to the transform in time and each additional component to the actual symbol (baud) is null at the sampling instant, cancelling or minimizing inter-symbol interference.

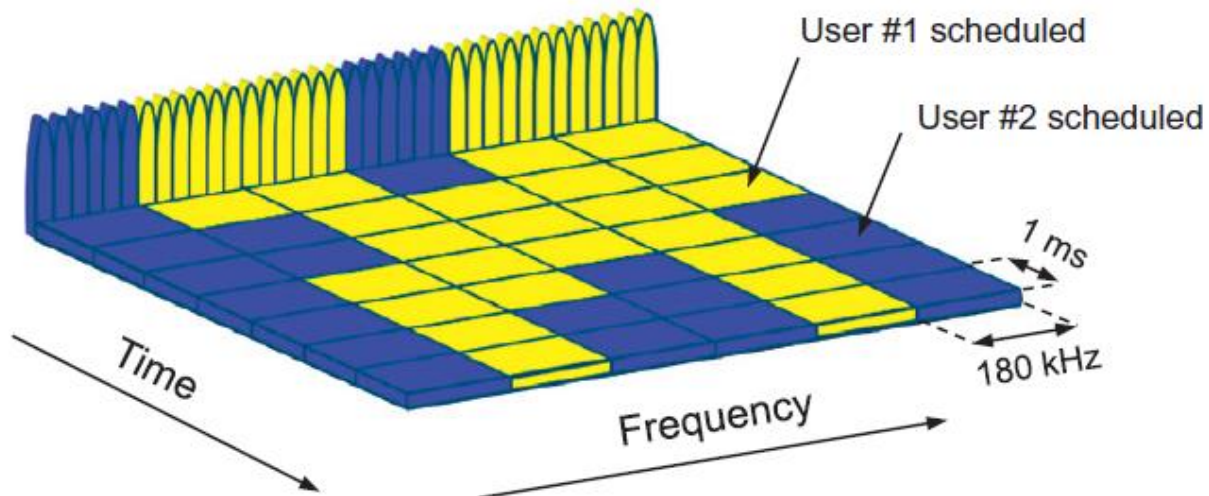


Figure D - 1. OFDMA Downlink channel programming in time and frequency domains in LTE (Dahlman et al [8]).

- VoIP services capabilities over IMS domain with QoS: VoLTE.
- Adaptive FEC Turbo coding together with QPSK, 16QAM and 64QAM modulation according to downlink/uplink quality.



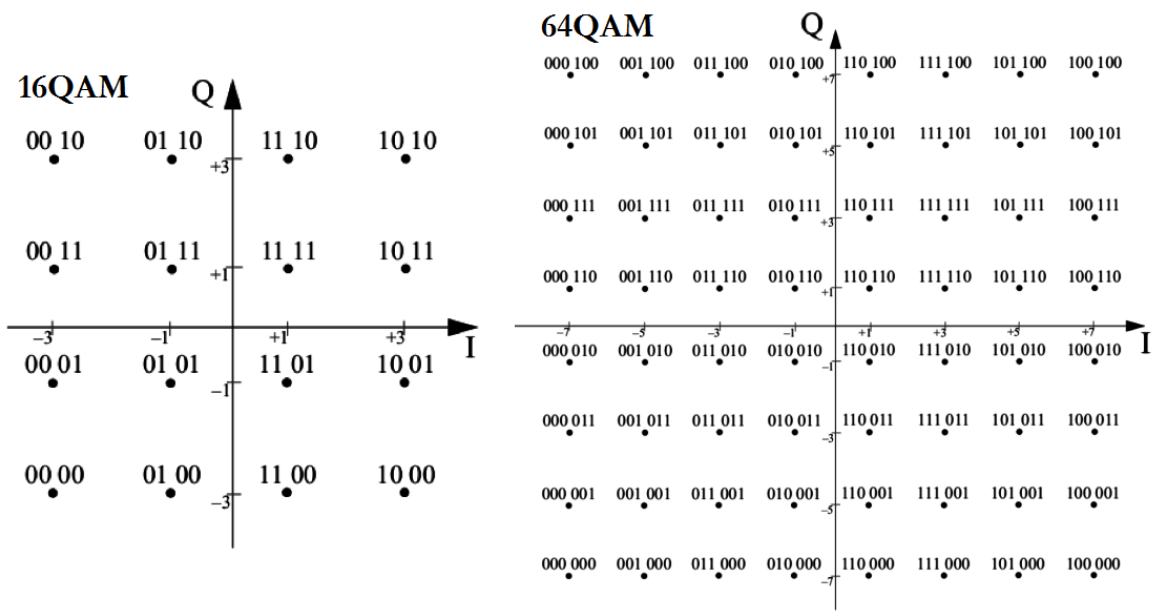


Figure D - 2. 16QAM and 64QAM constellations.

- Link adaptive power control.
- High spectral efficiency in LTE-UE connection and handover (optimum at 15 Km/h, supported as far as at 350 Km/h) and better control plane performance, with latencies lower than 10 and 50 milliseconds in the user and control plane respectively.
- New mobile equipment (LTE-UE), optimized for IP services.
- Interoperability with legacy GERAN and UTRAN and migration of those to LTE. Commitment of service during roaming among them via (Single Radio Voice Call Continuity) or CSFB (Circuit Switched Fall-Back).
- EPS uses «EPS Bearers» for routing traffic from a PDN Gateway towards a UE. An EPS bearer comprises an IP flow with QoS defined between the Gateway and the UE. Together, the E-UTRAN and the EPC establish and release EPS bearers on demand by the applications. Multiple EPS bearers might be established to a single user in order to providing different QoS to distinct PDNs (e.g. a user could be within a VoLTE call and simultaneously downloading a Web page through HTTP o transferring files via FTP).
- The EPS must provide security and privacy for protection of the user over fraudulent use.

LTE initial releases main characteristics						
Frequency Range	UMTS FDD and UMTS TDD					
BW de Canal 1 resource block (RB) = 180 KHz	1.4 MHz	3 MHz	5 MHz	10 MHz	15 MHz	20 MHz
	6 RB	15 RB	25 RB	50 RB	75 RB	100 RB
Modulation Scheme	Downlink	QPSK, 16QAM, 64QAM				
	Uplink	QPSK, 16QAM, 64QAM (optional at the UE)				
Multiple Access technology	Downlink	OFDMA ( <i>Orthogonal Frequency Division Multiple Access</i> )				
	Uplink	SC-FDMA ( <i>Single Carrier Frequency Division Multiple Access</i> )				
MIMO ( <i>Multiple Input - Multiple Output</i> )	Downlink	Wide range of MIMO configuration options for diversity of transmission option, special multiplex and cyclic delay (maximum of 4 antennas at the eNB and UE)				
	Uplink	Collaborative multi-user MIMO				
Peak Data Rates	Downlink	150 Mbps (UE category 4, 2x2 MIMO, 20 MHz) 300 Mbps (UE category 5, 4x4 MIMO, 20 MHz)				
	Uplink	75 Mbps (20 MHz)				

Table D - 1. LTE initial releases main characteristics.

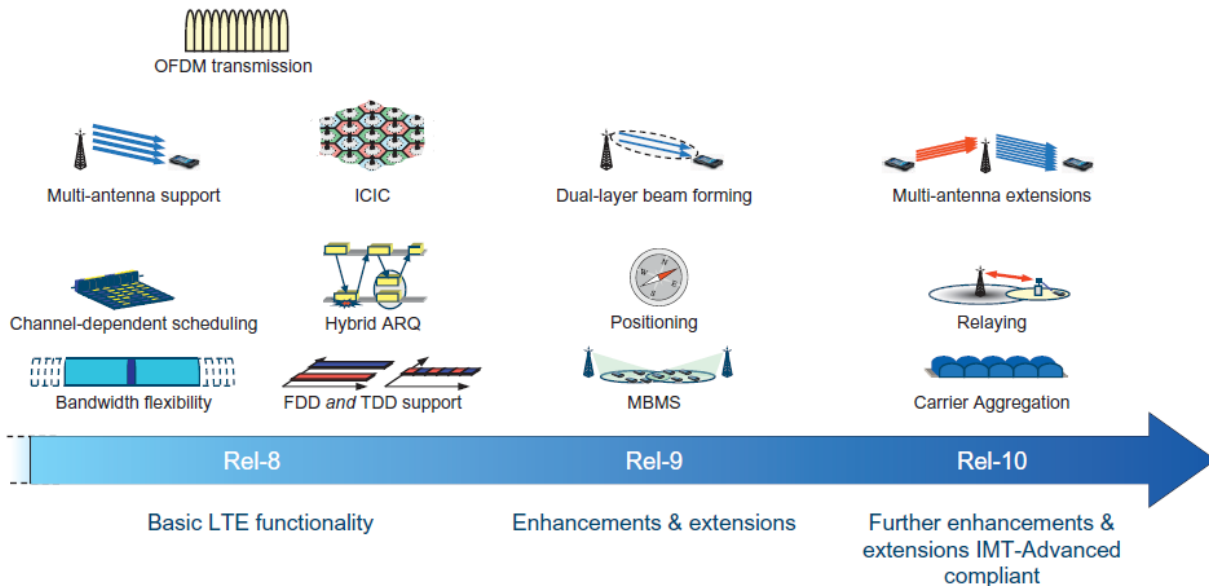


Figure D - 3. LTE/LTE-Advanced evolution as per 3GPP Releases 8 to 10 (Dahlman et al [8]).

## D.2 Network Architecture

UMTS evolution to LTE takes place in two areas:

- Evolved Packet Core Network (EPC). Natural evolution response to worldwide trend towards applications residing in packet-switched networks (Internet). EPC supports convergence of services based on asynchronous and real time packet-switching (VoIP).
- Evolved UMTS Radio Access Network (E-UTRAN). Responds to wireless higher bandwidth demands. E-UTRAN offers high speed, low latency and packet optimized access.

As for 3GPP's jargon, E-UTRAN is referred to LTE while EPC as SAE (System Architecture Evolution). UMTS evolution (LTE+EPC) is referred as EPS (Evolved Packet System).

### D.2.1 Evolved Packet Core (EPC)

EPC nodes are briefly described next:

- **Mobility Management Entity (MME)**. Control plane node involved in processing signaling between the UE and the CN. Protocols are named NAS (Non-Access Stratum), so that functionality between EPC and UE is split from the AS (Access Stratum) -which manages functionalities between the UE and the radio access network-.

The MME carries out several functions which can be discriminated into the following:

- Bearer management related functions (NAS protocol session management layer):
  - ✓ Bearer establishment, support and release.
- Functions related to connection management (NAS protocol connection and mobility management layers):

- ✓ Security procedures (authentication and cyphering).
- ✓ IDLE-ACTIVE transitions of Terminal-Network sessions (connection establishment and QoS).
- ✓ Mobility (UE paging)

- **Serving Gateway (S-GW).** User plane node that connects the EPC with the E-UTRAN. It anchors the user plane for mobility among different LTE access base stations (eNodeB), as well as other 3GPP type of access (GERAN, UTRAN/HSPA+, etc.).

The S-GW holds bearer information when the UE is in idle state and temporally stores downlink data while the MME initiates UE paging procedures for reactive them.

Additionally, the S-GW performs administrative functions such as:

- ✓ Collection of traffic/data volume statistic information for billing purposes.
  - ✓ Lawful interception.
- **Packet Data Network Gateway (PDN-GW or P-GW).** Basically, it connects the EPC with other PDNs such as Internet. Additionally:
    - ✓ Assigns an IP address to the UE.
    - ✓ Assigns QoS and volume based charging/billing information based on policies established at the PCRF. It then enforces QoS to guaranteed bearer's bit rates, as well as IP packet filtering among different EPS bearers according to QoS policies.
    - ✓ Anchors the user plan for mobility among 3GPP and non-3GPP systems (cdma2000, WiMAX, etc.).
  - **Policy and Charging Rules Function (PCRF).** Analogue to the one existing in UMTS IMS, but adapted to EPC. The PCRF manages the rules for determining the access and resources use by the user, as well as billing according to the PCEF (Policy Control Enforcement Function) residing at the P-GW.

PCRF also provides QoS authorization (QoS class identification and data rate) which decides how a specific data flow will be treated at the PCEF, assuring consistency with the user’s subscription profile.

- **Home Subscriber Server (HSS).** Analogue to the one existing in UMTS IMS, but adapted to EPC. It stores SAE subscription information such as EPS subscription QoS profile, roaming restrictions, PDNs to which the subscriber can establish according to an APN (Access Point Name label following DNS conventions) or PDN address (subscribed IP addresses). It integrates the AuC node, which stores authentication and security keys.
- **Evolved Packet Data Gateway (ePDG).** Its main function is assuring data transmission between the UE attached to an EPC over a non-reliable non-3GPP access. The ePDG acts as a termination sub-layer of an IPsec tunnel established up to the UE and the network’s edge.

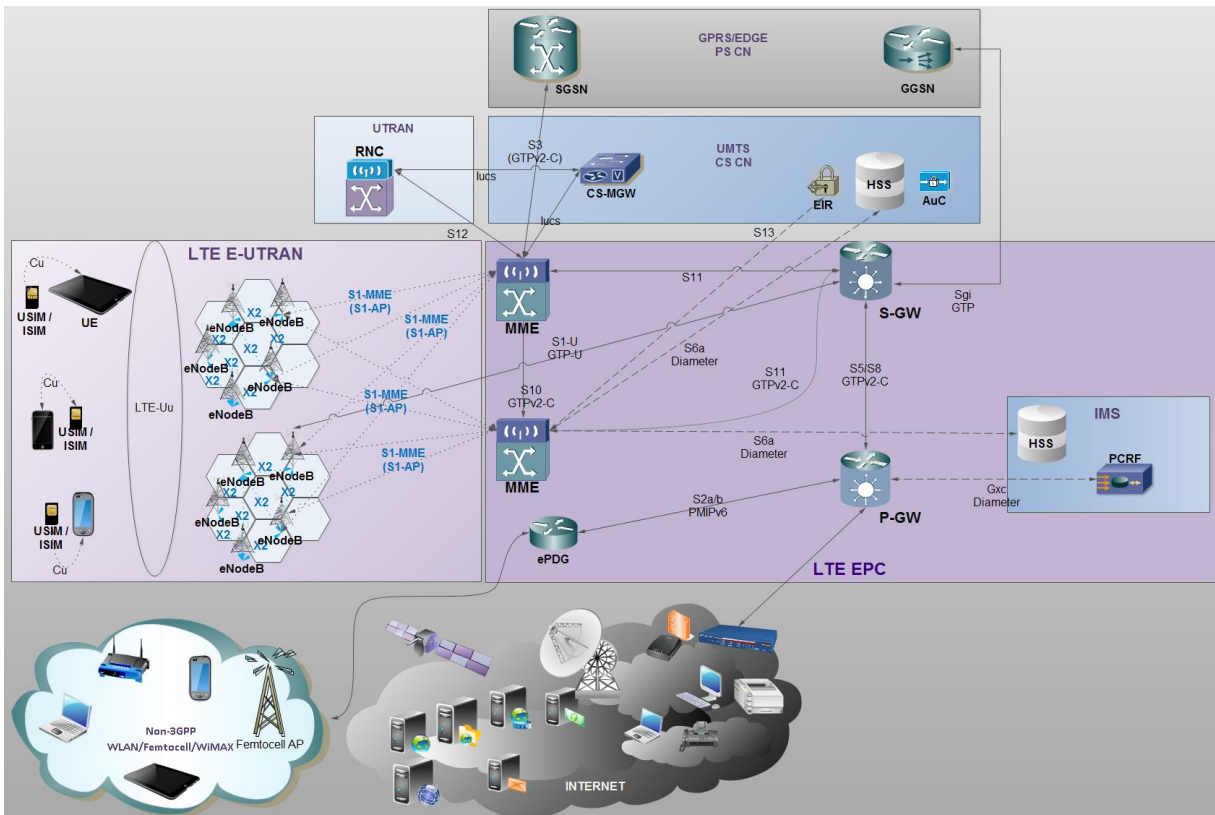


Figure D - 4. EPS (LTE+SAE) internetworking.

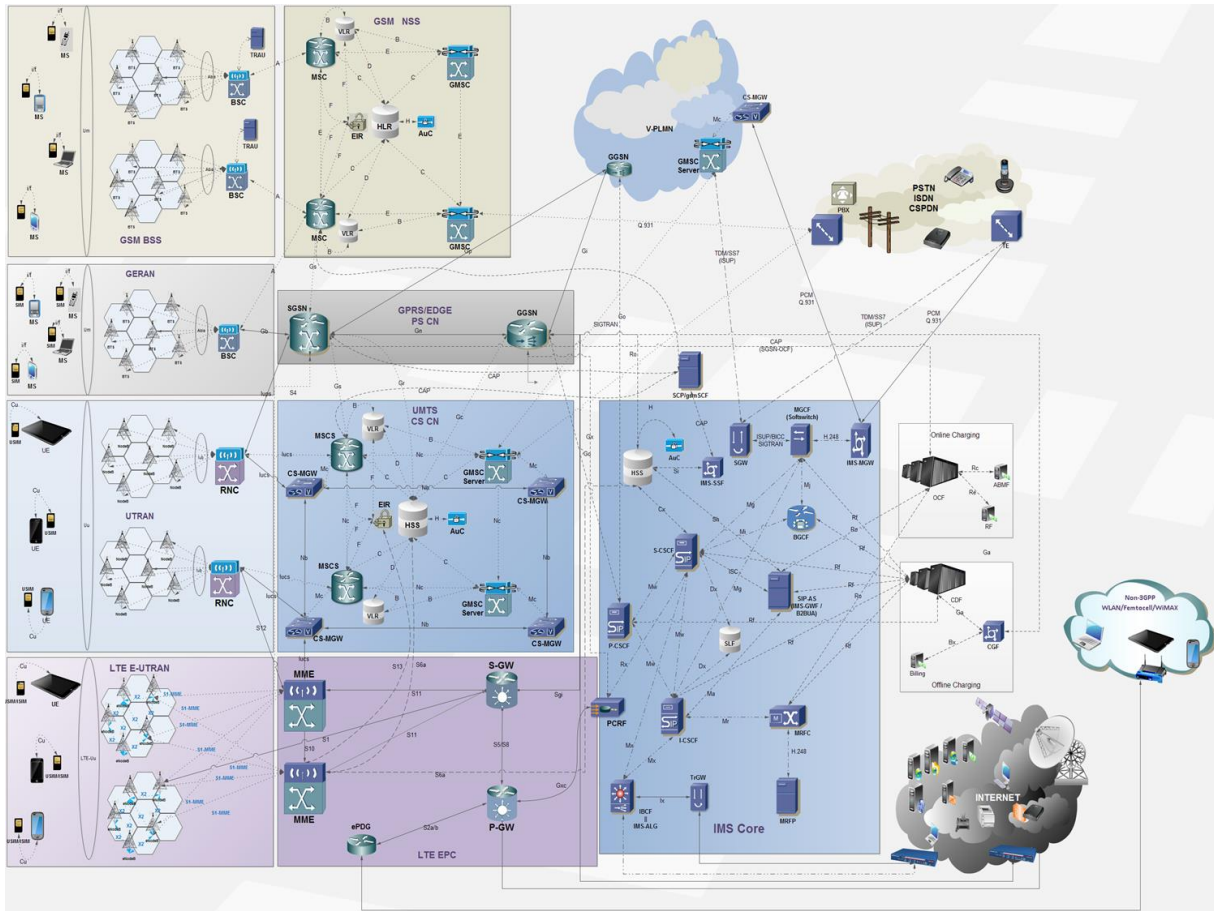


Figure E - 3. Internetworking GSM/GPRS/UMTS/IMS/LTE.

### D.2.2 Evolved UMTS Radio Access Network (E-UTRAN)

The E-UTRAN is composed by the evolved base stations or eNodeB (**eNB**), which implement all radio access related functions, namely:

- Radio Resource Management (**RRM**). Covers all functions related to radio bearers, such as carrier control and admission, mobility, scheduling and dynamic resource assignment to UE in either directions (Downlink/Uplink).
- Header compression. By reducing the overhead, it aids the radio interface by reducing overhead, mainly in short packages like the ones carrying voice (VoLTE).
- Security. All information conveyed over the radio interface is encrypted.

- Connectivity with the EPC. Consisting in signaling towards the MME and the bearer path towards the S-GW.

The eNBs are capable of managing several cells. Contrarywise to preceding RANs (GSM BSS, GERAN, UTRAN), there isn't a controller node (BSC or RND) within E-UTRAN, as their functions are integrated in the eNBs. Consequently:

- ✓ Latency is reduced ⇒ efficiency is enhanced.
- ✓ Point of failure and costs are reduced.
- ✓ As the UE moves ⇒ whole information or «UE context» is transferred among eNBs (together with other eventually stored data) ⇒ mechanisms are implemented for avoiding data loss during handoffs.

The protocols conveyed in the LTE-Uu interface (eNB – UE) are known as AS (Access Stratum).

The eNBs are connected through the X2 interface, meanwhile they connect to the EPC via the S1-MME and S1 (also named S1-U) towards the MME and S-GW respectively.

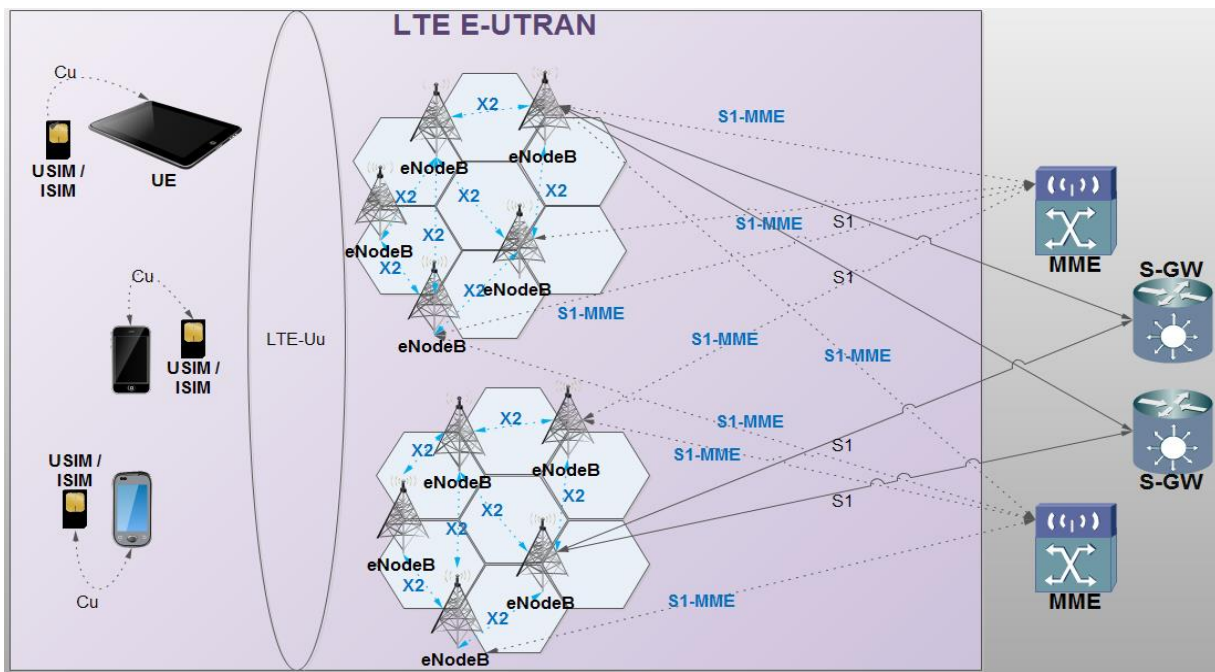


Figure D - 5. LTE E-UTRAN interfaces.



«S1-flex» is a concept by which multiple MME/S-GW may give service to a common geographical area, being connected by a mesh network to the eNB set of such area. An eNB is then a client of several MME/S-GW serving a «pool area». The set of such MME/S-GW is known as «MME/S-GW pool». This concept implies:

- ✓ Processing load sharing
- ✓ Improved robustness by eliminating single points of failure.

Normally, the UE remains with the same MME while is located within the pool area.

### D.2.3 Network Architecture Interfaces Roles

Next figure shows the main roles carried out by LTE architecture interfaces, either within the E-UTRAN and EPC or with other PDNs like the IMS, GPRS or the accounting/billing domain namely:

- Accounting/Billing Management.
- Access/Mobility Management.
- Bearer/QoS Management.
- User Traffic.

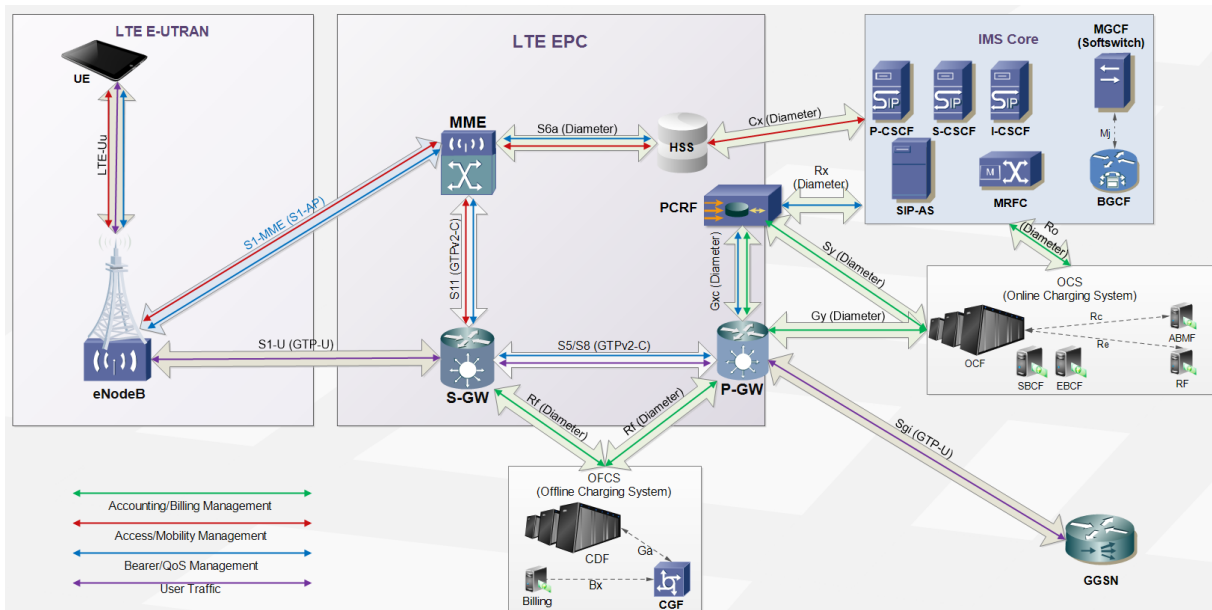


Figure D - 6. LTE interfaces roles.



## D.2.4 LTE User Plane Protocol Stack

An IP («Internetworking Protocol») packet for the UE is embedded in an EPC-specific protocol and conveyed within a tunnel between the P-GW and the eNB. Different tunneling protocols are used among different interfaces. S1 and S5/S8 use GTP.

E-UTRAN user plane protocol stack consists of «Packet Data Convergence Protocol» (PDCP), «Radio Link Control» (RLC) and «Medium Access Control» (MAC) sublayers which are terminated at the eNB at the network side.

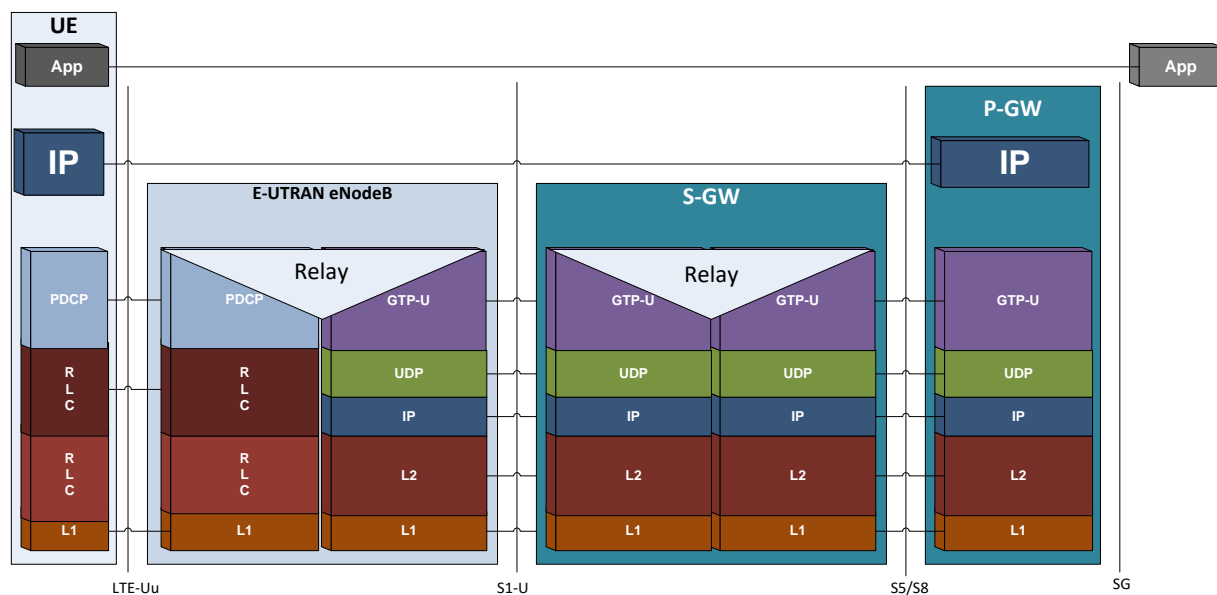


Figure D - 7. LTE User Plane Protocol Stack.

A brief description of these user plane protocols is described next:

- Internetworking Protocol (**IP**): resides in LTE-UE for providing services to the applications accessing the mobile terminal from different PDNs. IP is typically used with TCP and/or UDP (and occasionally, with SCTP).
- Packet Data Convergence Protocol (**PDCP**): main functions of PDCP include:

- Robust Header Compression (ROHC) of user's IP packets.
  - User and control plane encryption. NAS messages are encrypted both in the eNB and the MME, thus involving two encrypting processes.
  - Match different protocols PDUs before its segmentation and passage towards RLC in the bearers.
- Radio Link Control (**RLC**): it comprises a sublayer of similar procedures as the one in UMTS/HSPA for the transmission of interactive flows in real-time, like VoIP and videoconferences (given its low latency), upload or download of files, broadcasting information. These procedures are carried out in either of three modes: (Acknowledged), UM (Unacknowledged), y TM (Transparent).

RLC employs retransmission mechanisms for the sequential delivery of SDU (Service Data Units) to upper layers. RLC segments SDUs in an adaptive way according the radio link quality.

RLC connects with the MAC sublayer through logic channels controlled by RRC in NAS mode.

- Medium Access Control (**MAC**): simplified in LTE, given it avoids the proliferation of MAC entities, amassed in WCDMA. It contains the HARQ (Hybrid Automatic Repeat reQuest) function, which operates with multiple concurrent processes for increasing the data stream.

At eNB's downlink, HARQ operates with synchronous retransmissions that happened in predefined temporal instances within the frame streaming, without requiring explicit signaling towards the receiver. In the uplink, asynchronous retransmissions are used, which allow the scheduling of those according to the air interface conditions. At the LTE-Uu sublayer, MAC maps the logical channels (RLC-MAC) in transport channels (MAC-PHY), and is in charge of the traffic scheduling within these channels according to the priorities established by each UE, as well as the selection of the most adequate transport set-up. MAC scheduling resides in the eNB and operates in either transmission ways (D/U).

- **PHY** or L1: LTE-Uu air interface comprises the following processes:

- Turbo FEC (Forward Error Correction) and CRC;
- Transport channel mapping into physical channels;
- Octet and bit interleaving;
- Speed adjustments at the physical channel adaptation;
- OFDMA and SC-TDMA modems.

Other interfaces such as S1-U, S5/S8a y SGi, PHY might include base band drivers for the transport over 802.3 (Ethernet) at 100 Mbps or 1 Gbps.

### D.2.5 LTE Control Plane Protocol Stack

LTE's control plane protocol stack between the UE and MME is displayed in next figure. NAS protocol is discriminated, meanwhile AS are those of lower level at the LTE-Uu interface. The lower layers perform the same functions of the user plane with the exception that there is no header compression.

A brief description of these control plane protocols is described next:

- Non-Access Stratum (**NAS**):
  - Allows dialogues with EPC's MME.
  - Mobility and session management functions including:
    - ✓ Call control;
    - ✓ Authentication and security management;
    - ✓ AT command management (UE TE↔TA UE as for 3GPP TS 27.007).
- Radio Resource Control (**RRC**): known as «layer 3» in the AS protocol stack. It remains the main control function of the AS, being responsible of the establishment of radio bearers and the configuration of lower layers using RRC signaling between eNB and the UE. It provides:
  - ✓ System information broadcasting.
  - ✓ Configuration of PDCP, RLC and MAC sublayers.
  - ✓ Administrates radio resource management for mobility management.
  - ✓ Bearer services QoS.
  - ✓ Paging management.
  - ✓ Measurements and reports for the eNB.

- ✓ System information management.
- ✓ Cell selection and handoff management.
- ✓ Security and data authentication of the RRC layer.

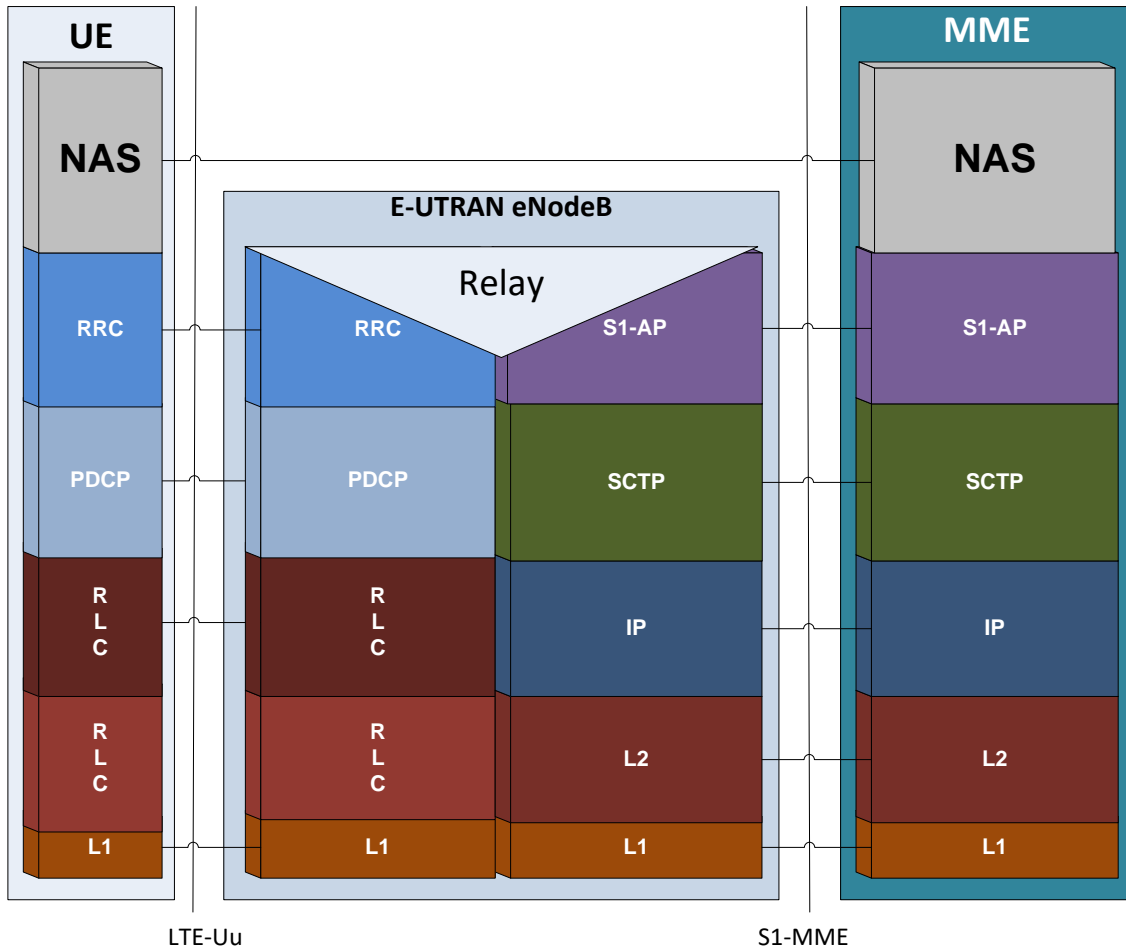


Figure D - 8. LTE Control Plane Protocol Stack

- **S1 Application Part (S1-AP):** it comprises the signaling service between eNB and MME through the S1-MME interface. S1-AP provides interface functions such as:
  - ✓ SAE management function provider.
  - ✓ Mobility functions.
  - ✓ Paging.
  - ✓ NAS transport

- ✓ Error reports
- ✓ State transfer.
- ✓ Reset functional services
- ✓ «UE context» decouple.

### D.2.6 NAS Procedures

«Non Access Stratum» procedures are conceptually analogous to those of the UMTS (especially the ones related to connection management). The main change remains in the fact that EPS allows procedures concatenation, thus allowing a more agile and fast establishment of connections and bearers.

From these procedures emerges for example the «**Initial Attach Procedure**» shown in next call flow diagram: the MME creates this context when the UE is turned on and attaches to the network. It assigns a unique temporal identity denominated S-TMSI (SAE - Temporary Mobile Subscriber Identity), which identifies the UE in the MME context. The «UE context» maintains user subscription information downloaded from the HSS.

The «UE context» information is hold in the MME during idle periods (where all resources are released).

«Initial Attach Procedure» is depicted in next call flow diagram, where the following steps are discriminated:

- i. UE initiates registration procedure with the network. The MME assumes responsibility with the assistance of the HSS/AuC and EIR.
- ii. The user is authenticated.
- iii. The UE is validated.
- iv. Location update in the HSS («UE context»).
- v. MME initiates «Default Bearer» activation.
- vi. P-GW requests charging rules and policies to the PCRF and available credit at the OCS.
- vii. MME ends activation procedures and data start flowing.

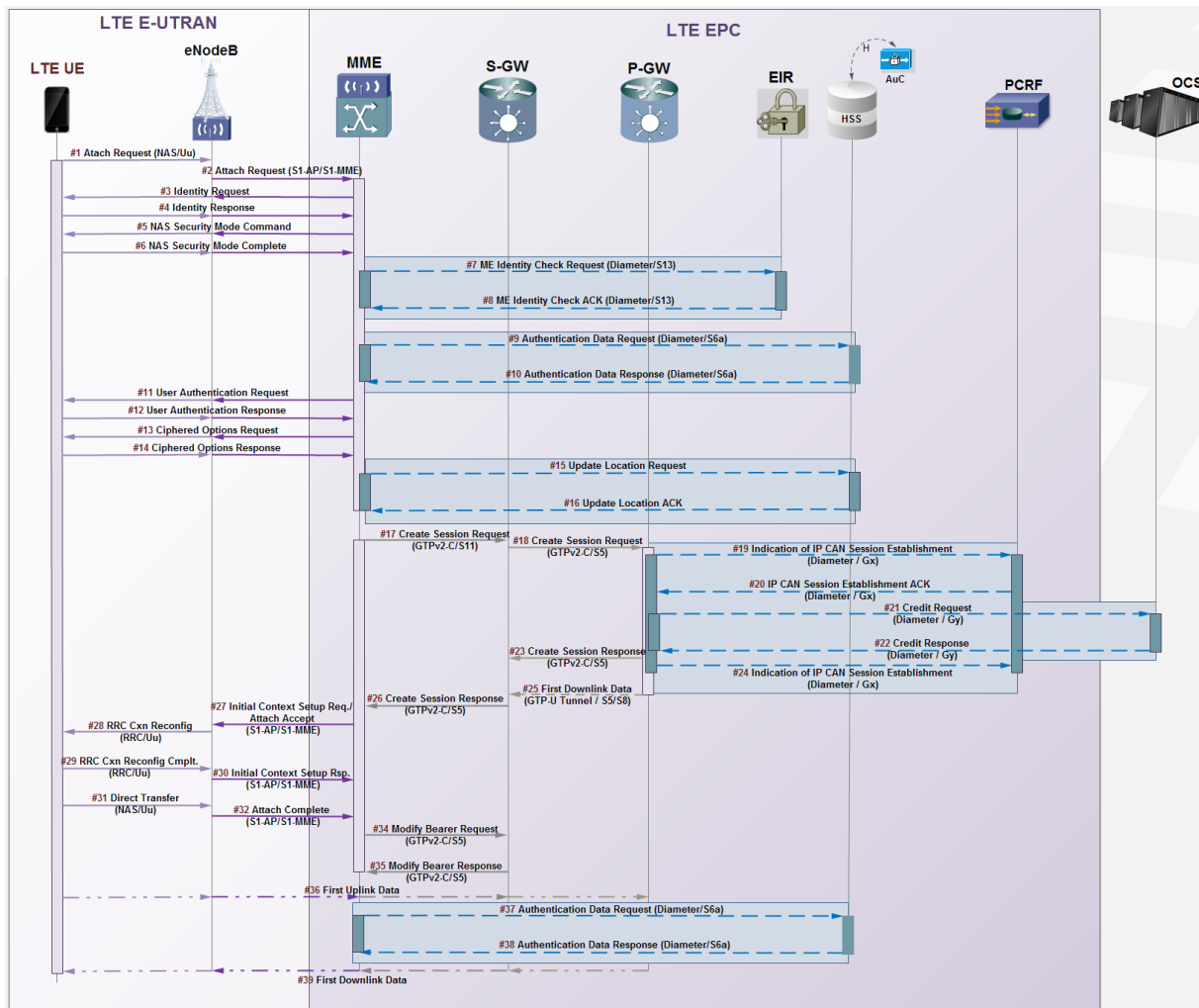


Figure D - 9. LTE Initial Attach Procedure.

«Tracking Area Update»: another NAS for allowing the network contacting an idle UE («ECM-IDLE»); the UE updates the network every time it moves away from the TA («Tracking Area»).

The MME is responsible of tracking the user's location during the idle period through paging messages to all eNBs in the TA over the air interface, as well as the «UE context» reestablishment and radio carriers during transitions to active status or «ECM-CONNECTED» (e.g. when it is necessary to deliver information to an idle UE).

Security functions are responsibility of the MME either for the user or control plane. When a UE attaches to the network, a mutual authentication occurs between the UE and MME/HSS (the latter establishes the security keys used for bearers encryption).

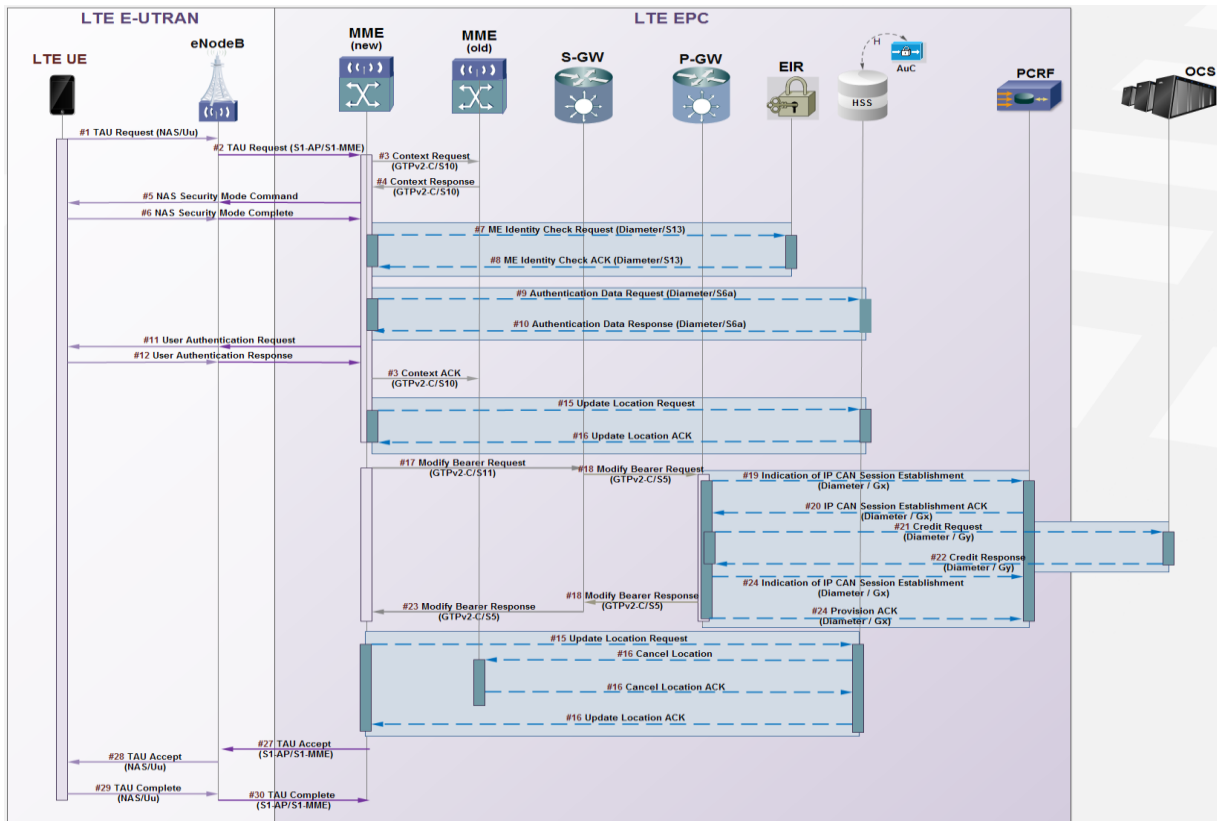


Figure D - 10. LTE Tracking Area Update.

### D.2.7 High Level Control Plane Protocols

EPS Mobility Management (**EMM**): EMM provides support to UE mobility in the E-UTRAN, as well as security control by several procedures:

- EMM Common Procedures: performed all the time as long as a NAS connection exists. They provide authentication, identity, security mode control, GUTI (Globally Unique Temporary ID) reallocation.
- EMM Specific Procedures: applied to one UE at a time and comprise UE attachment and detachment, and periodic and combined TA update.

- EMM Connection Procedures: they manage the UE connection with the EPC and provide support for service requests initiated by the UEs, the paging procedures towards the UEs, the bidirectional transport of generic NAS messages or those containing SMS.

EPS Session Management (**ESM**): used for session establishing with the UE and EPS bearer's context support. It provides user plane bearers control for permanent session along with AS control. ESM generates transactional messages for its operation, except while the attachment process or during EMM transactions.

ESM procedures are possible if there is an EMM context with the UE at the MME having already happened the authentication phase under secure NAS messages (initiated by the MME through EMM transactions).

ESM supports EPS bearer's context Management (activation and deactivation of default EPS context, dedicated EPS bearer contexts and processes for the modification of already established EPS contexts). It also supports associated transactional processes initiated by UE request, either for establishing or releasing sessions with PDNs or managing, modifying or releasing dedicated bearer resources.

Next call flow diagram illustrates the «**Dedicated Bearer Activation Procedure**», consisting of the following main steps:

- i. UE attempts to access to an IMS service.
- ii. AF notifies the PCRF.
- iii. PCRF sends QoS determination to the P-GW.
- iv. P-GW initiates dedicated bearer activation towards the eNB (after inquire to OCS).



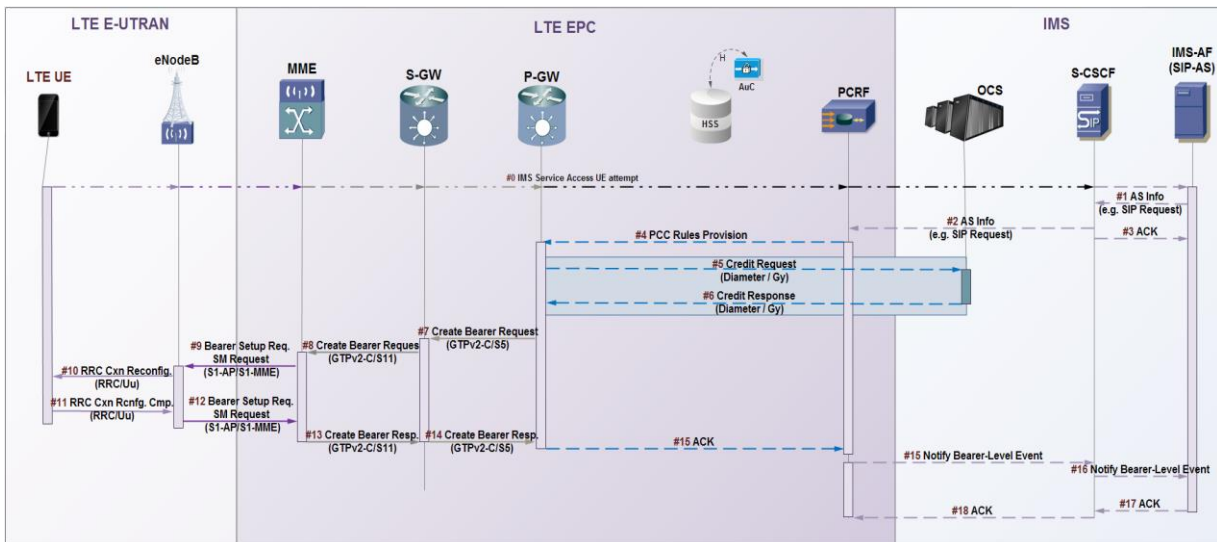


Figure D - 11. LTE Dedicated Bearer Activation Procedure.

### D.3 VoLTE and LTE services

Classic mobile telecommunication services such as voice, messaging, location, etc., are accomplished on the long term by using signaling protocols such as SIP (VoLTE, IM, USSI) and Diameter (AAA extensions, QoS, LCS, etc.).

Depending on the reached level of LTE deployment, voice service is accomplished within LTE access through the following methods:

**CSFB** (Circuit-Switched Fall Back): a displacement to legacy Circuit-Switched is accomplished for voice service provision. Main disadvantage of this approach is the impossibility of simultaneous access to voice and data access via LTE.

**SRVCC** (Single Radio Voice Call Continuity) is the term used whenever LTE access is lost and a CSFB must be performed for not dropping the established call. Hence, SRVCC allows roaming in non-LTE networks.

**VoLGA** (Voice over LTE Generic Access): enables mobile devices to access legacy network services without losing LTE access by using an emulation principle through which the LTE network appears as a BSC/RNC from a MSC/MSCS

perspective, appearing as a mobile application from the LTE-UE perspective. Legacy messages for call control are encapsulated within a tunnel towards and from the LTE mobile device.

According to 3GPP TS 23.879, VoLGA uses an IWF (Interworking Function), also known as **VANC** (VoLGA Access Network Controller), interleaved between the EPS and the MSC(S), which provides an access relay tunnel to LTE from the UE to the MSC(S). Signaling for legacy CS CN as the ones used in GSM/UMTS is conveyed seamlessly from LTE to the VANC, where shift to A/Uu interfaces is done for transport towards the MSC(S). It is important to notice that VoLGA will soon be deprecated and it does not follow 3GPP/LTE specification guidelines but VoLGA Forum's.

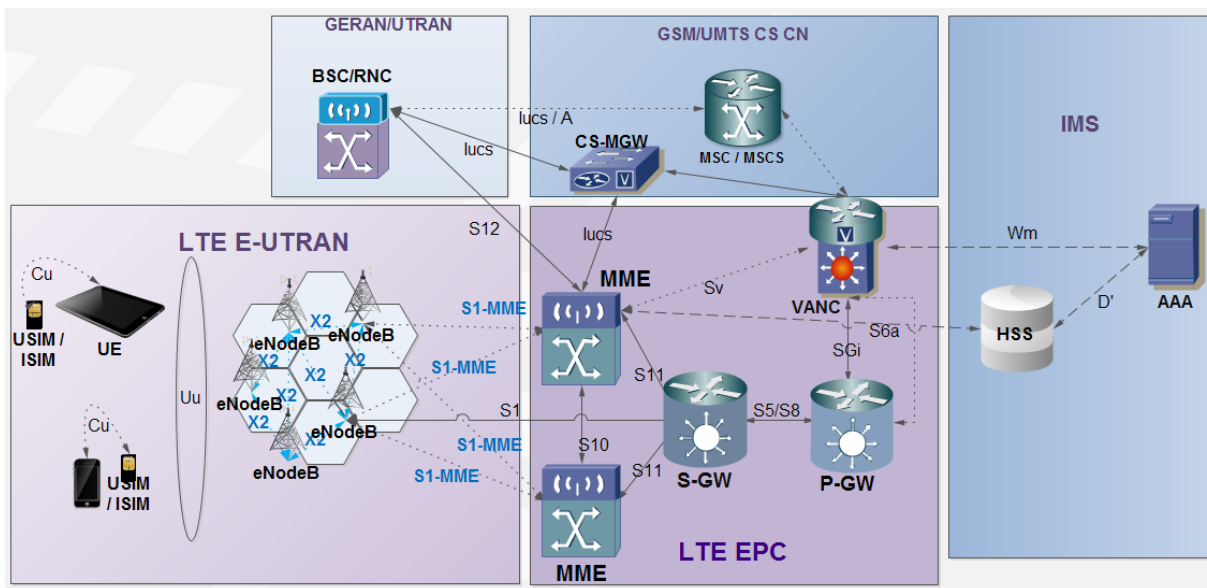


Figure D - 12. VoLGA internetworking.

**VoIMS** (Voice over IMS) is the 3GPP/LTE method for pure VoLTE. It only uses nodes of the EPS and IMS architecture and, consequently, call control and AAA protocols for LTE and the IMS, i.e. SIP and Diameter (and RTP/RTCP in the user plane). Steps for establishing a VoLTE call are described next:

1. UE Authentication. Procedure carried out between the eNB and the MME together with the HSS and the AAA server. Once authenticated, EPS bearers may be established.
2. Signaling for PDN Default Bearer establishment. The MME establishes the path between the eNB and the PDN or Internet. Then, it selects the EPC' S-GW and P-GW nodes for accessing services in either environments.
3. Signaling for IMS Default Bearer establishment. Same as in 2, but for the IMS Bearer.
4. Registration to the IMS via SIP. The UE registers to the IMS by sending a SIP REGISTER message to the IMS via the IMS Default Bearer (refer to annex E for SIP REGISTER description).
5. Register inquire. After SIP registration, the CSCF must query the HSS and the AAA Server via Diameter, so as to assuring identity, state and authorized services.
6. Subscription to Services. Through a SIP SUBSCRIBE message from the UE to the IMS via the IMS Default Bearer, the UE may subscribe to presence service, so as to noticing about other users connectivity and its own.
7. Status/presence change notification. Through a SIP NOTIFY message sent from the IMS towards the UE via the IMS Default Bearer, the user can notice the connection of a user to whom making a call.
8. Internet access. Through the Internet Default Bearer, the user may access to WWW services (e.g. Facebook).
9. VoLTE call establishment. Via a SIP INVITE message, sent from the UE to the IMS via the IMS Default Bearer, the UE might initiate a call or multimedia session.
10. VoLTE call signaling bearer. The PCRF and MME establish an additional bearer in the control plane through the network for the VoLTE call.
11. VoLTE call QoS configuration (RTP/RTCP in user plane). After the SIP INVITE reception, via Diameter a dialog is carried out with the PCRF to establish the call's appropriate QoS (e.g. Quality Control Index -QCI- set to 1 for maximum latency of 100 ms).

12. VoLTE call established between users. Through SIP signaling in the control plane and RTP/RTCP in the user plan over UDP (voice does not traverse the CSCF in the IMS), the call is maintained in the IMS as long as it takes taking into account topics involving statistics, security, accounting, etc.

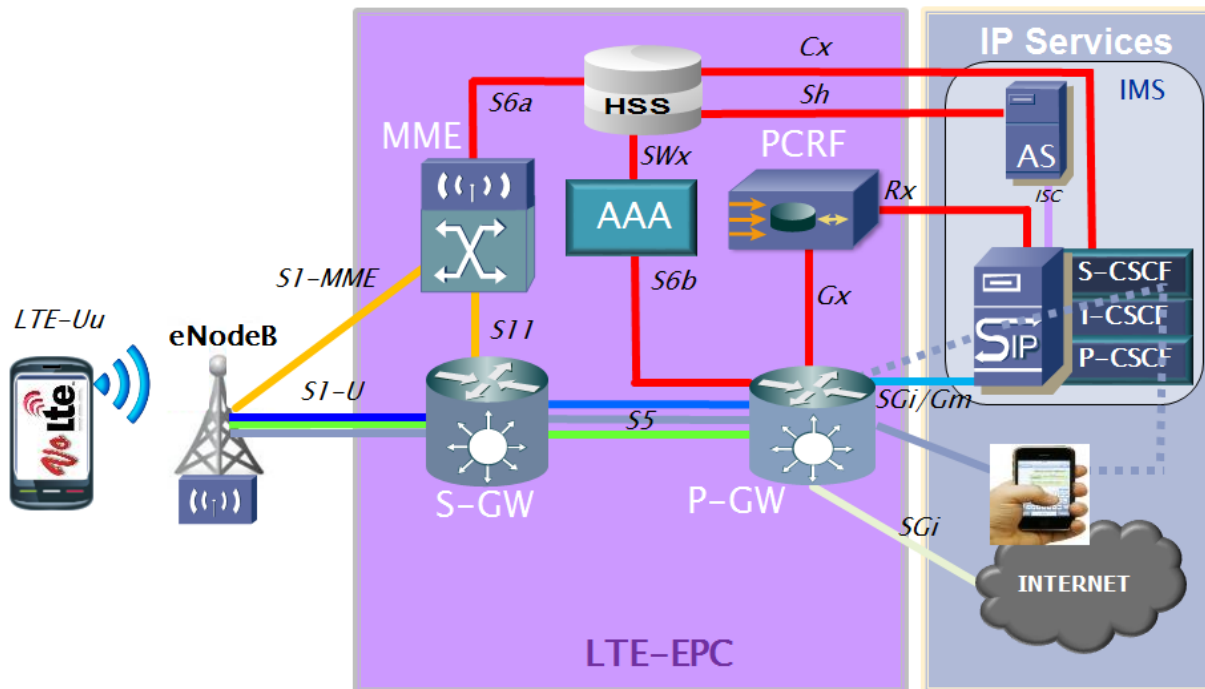


Figure D - 13. VoLTE traversing E-UTRAN, EPC and IMS (VoIMS).

For further comprehension of VoLTE and the procedures aforementioned, annex E and F need to be reviewed. Figures F-18 and F-19 complement Figure D-13.

## D.4 LTE-Advanced

LTE-Advanced objectives are established by 3GPP/LTE beyond Release 10 technical specifications (started in 2011) and subsequent releases until reaching IMT-Advanced specification parameters. Other organisms such as IEEE and WiMAX Forum have been developing IMT-Advanced specifications around IEEE 802.16e

(Mobile WiMAX). These groups and related are developing specifications for the interoperability of IMT-Advanced systems such as LTE-Advanced and WiMAX 2 (IEEE 802.16m). Either technologies make extensive use of OFDMA, MIMO, Turbo coding, intelligent scheduling, links adapted to the radio channel quality and relaying.

Initial focus of 3GPP/LTE for LTE-Advanced is centered in obtaining an improved performance and capacity by the following objectives:

- Duplicate spectral efficiency of Release 8 specs.
- Retro-compatibility with Release 8 by using new features such as Carrier Aggregation (CA) which allows using up to five LTE R8 frequencies (1.4, 3, 5, 10, 15 or 20 MHz) and therefore reaching bandwidths of 100 MHz per operator and speeds up to 3 Gbps in the downlink, meanwhile each frequency component is retro-compatible with LTE R8. LTE-Advanced employs this mechanism either in FDD and TDD and even more, allow total bandwidths in each direction to be different according to the quantity and type of component added. This gives flexibility to either downlink and uplink throughput as needed for a particular network.
- Mobility support of UE within the network up to 350 or 500 Km/h depending on the used frequency.
- A significant increase of simultaneous subscribers per cell, greater than 500% of LTE R8.
- Performance enhancement at cell edges by using MIMO technologies for obtaining equivalent LTE services quality across the entire LTE coverage. LTE-Advanced increases spectral efficiency by supporting MIMO 8x8 schemes in the downlink, for a maximum of 30 bps/Hz, and MIMO 4x4 in the uplink for a spectral efficiency of 15 bps/Hz. LTE R10 introduces DM-RS (Demodulation Reference Signal), which are added to each flow before its pre-coding, which allows the receiver to discriminate the pre-codec without previous information or Codebooks.
- Dynamic optimization of all access network resources through Relay Nodes, enabled to support route swapping within the own RAN for a better efficiency in

the connectivity of LTE terminals with the EPC. By the use of RNs, which comprise low power base stations, the following objectives are accomplished:

- ✓ Improve coverage in cell edges with medium or high traffic load by providing high quality links.
- ✓ Remote areas coverage by using an LTE-based wireless backhauling, without the need of dedicated microwaves or fiber links.

The remote RN uses a new air interface: Un, by which it connects to an eNB whose role is being the donor eNB. The Un interface is an LTE-Uu E-UTRAN interface modified for supporting in dedicated mode the user traffic between the eNB and the RN. The radio resources of the donor eNB are shared between the UEs served by the donor eNB (DeNB) and the RN,

## Annex E

### E Voice Over IP Overview

#### E.1 Introduction to VoIP

VoIP derives from Voice over IP or Voice over Internet Protocol. VoIP allows media (audio/video) being transported over IP packets and, consequently, through Packet-Switched networks as Internet or MNO PS CN (GPRS/EDGE, UMTS's IMS or LTE -VoLTE-). It comprises the foundation of the IP Telephony paradigm shift, then converging two historically separate ecosystems: voice and data transmission.

VoIP does not constitute a service by itself but a technology composed by:

- Multiple protocols either for the control and user plane (signaling and media respectively).
- Multiple network topologies (e.g. IMS).
- Multiple devices (codecs, handsets, etc.)

This technology allows encapsulating media (voice/video) in packets to be transported in data networks without the need of conventional Circuit-Switched networks as the PSTN or first generation PLMNs (GSM/IS41/IS-95, etc.), deployed over decades with the sole purpose of transmitting voice with an outstanding quality of service.

Either the PSTN or first generations of PLMN, where based on Circuit-Switched Core Networks. Hence, a communication requires the establishment of a

physical circuit during its entire duration. This fact demands that resources occupied during the communication cannot be used for any other matter until the communication is released. On the other hand, IP telephony is based on packet switching, i.e. transmits multiple conversations through the same physical channel, encoded in packages and independent flows.

Given the formidable quality of service, robustness and universality of classic telephony over circuit-switched networks, one question arises: why VoIP? Due to many factors, namely:

- Voice, video and data integration.
- Bandwidth consolidation.
- More cost-effective use of channels by harnessing the intervals between frames.
- Telecommunication costs.
- Rising advantage of packetized media in terms of costs.
- Internet's universal presence.
- TCP/IP protocol stack resides even in user's PC's.
- Technology maturity.
- Digital Signal Processors development for high speed Codecs and Modems.
- Shift of services towards data networks.
- More than 80% of services transmission over packet-switched networks and rising.
- Rising influence in long distance communication.



- Settlement of new paradigms imposed by the Service-Oriented Architecture (SOA) and Next Generation Networks (NGN).

Basically, a VoIP network proceeds with the following steps for communication means:

- I. Both endpoints register at the VoIP server.
- II. Via the VoIP server, the transmitting endpoint investigates communication characteristics at the receiving endpoint via a signaling protocol (SIP, H.323, H.248, etc.).
- III. The VoIP server returns the contact details to the transmitter.
- IV. A Codec is negotiated between ends (G.711, G.729, GSM, etc.).
- V. Digitization of the media (audio/video) in data packets.
  - a. Analog/Digital conversion via Codec.
  - b. Compression algorithm.
  - c. Digital framing.
- VI. Transmission over the IP network.
- VII. Conversion of the digitized media at the destination through the inverse steps carried out at the transmitter.

## E.2 Basic components of a VoIP network

Three basic components exist in a VoIP network, namely:

- **Client.** Establishes and terminates calls. Codes, packetize, and transmits the analog information. Likewise, decodes and reproduces the media information received.

- **Server.** It carries out operations of user validation, rating, accounting, billing, collection, profit distribution, routing, overall service management, customer load, service control, user registration and directory services.
- **Gateway.** It provides interfaces with traditional circuit-switched telephony, functioning as a platform for virtual clients. They also play an important role in access security, accounting, Quality of Service (QoS) control and the improvement thereof.

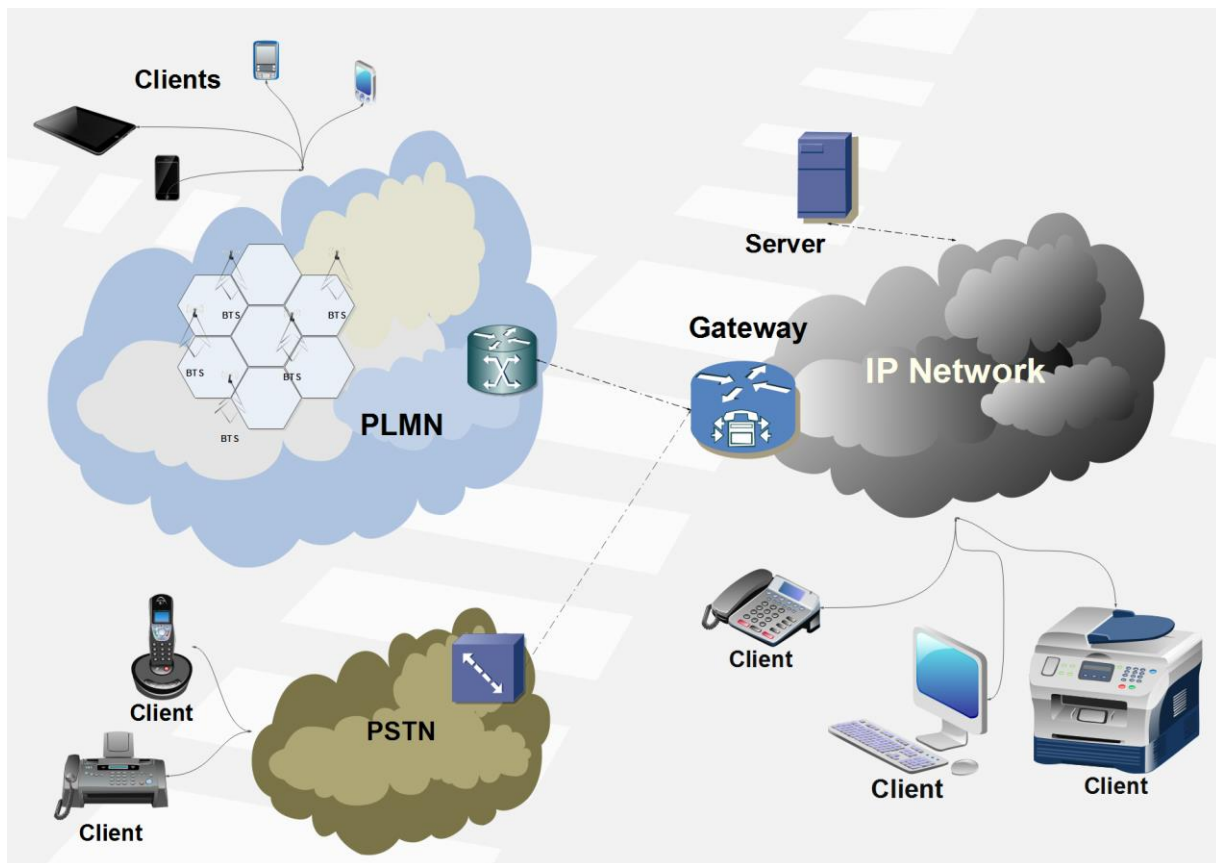


Figure E - 4. VoIP basic components.

Actually, many components exist in advanced voice/media networks over IP, as in the IMS or LTE. Next figure depicts as example of basic IMS components interworking with PLMN and PSTN. Nevertheless, these three components described here also constitute the main basic ones in every VoIP network.

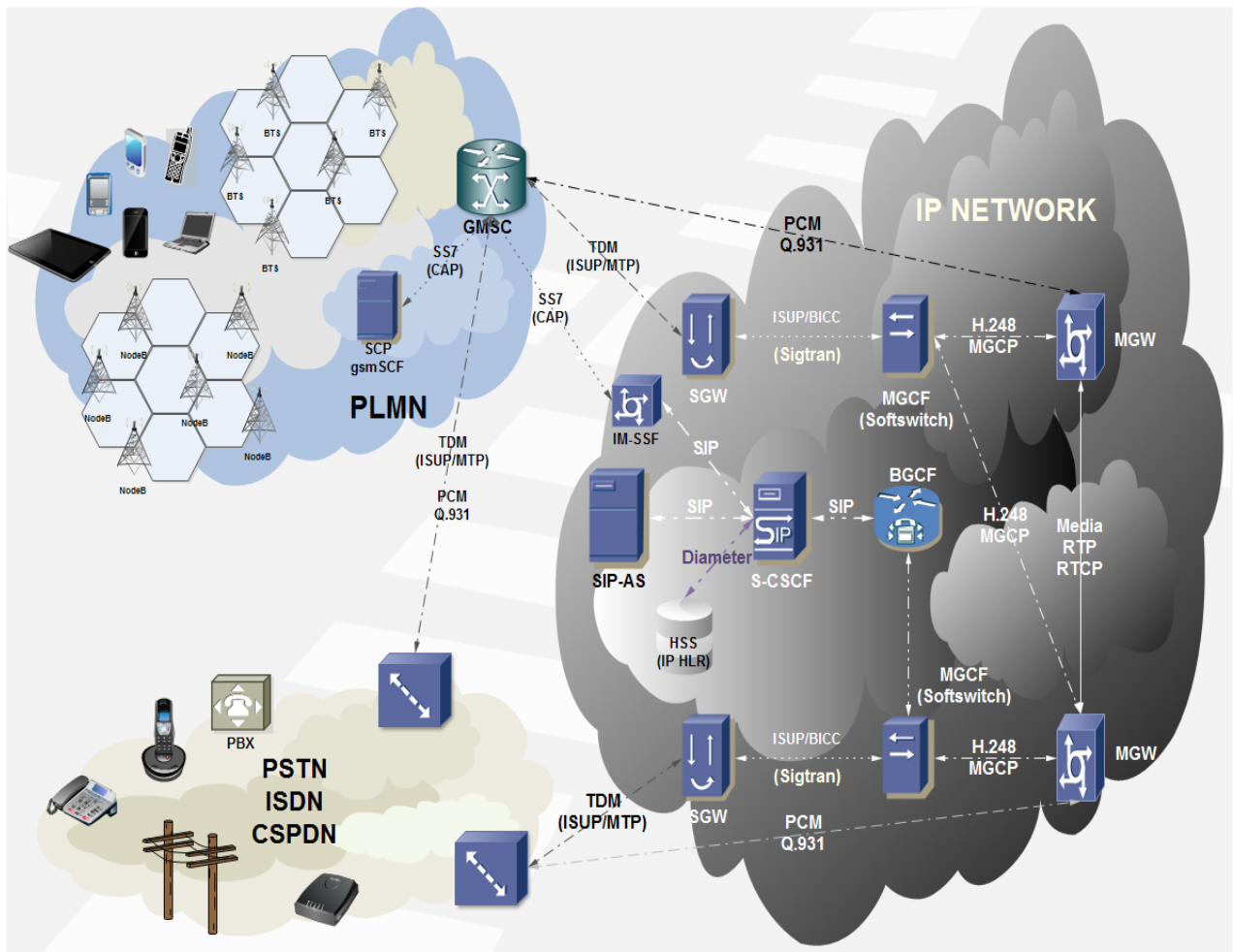


Figure E - 5. Basic IMS internetworking with CS CN like the PSTN or PLMN.

### E.3 VoIP Architectures

VoIP technology allows networks to be built under a centralized or distributed architecture. This flexibility allows building networks characterized by a simplified administration and terminal innovation, depending on the used protocols.

### **E.3.1 Centralized Architecture**

Mostly, a VoIP centralized network architecture is associated by MGCP and MEGACO (H.248) protocols. These were designed for a centralized entity named «Media Gateway Controller», which manages call switching and control logic.

Intelligence of the network is centralized and user equipment have limited characteristics.

Main benefits of this architecture approach is its centralized administration, call provisioning and control, simplifying the call flow by voice characteristics recurrence.

### **E.3.2 Distributed Architecture**

A VoIP distributed network is associated with SIP and/or H.323 protocols. These protocols allow intelligence to be distributed among the network between call control entities and terminals. Intelligence in this instance is referred to call establishment, characteristics, provisioning, billing, or any other aspect of call management.

Terminals might be VoIP Gateways, IP phones, media servers, or any device enabled to initiate and release a VoIP call.

Call control entities are denominated Proxy/Redirect Servers in a SIP based network, or Gatekeepers under an H.323 network.

## **E.4 Control and User Planes in VoIP Networks**

As in traditional telephony, VoIP includes a control plane, where signaling messages are carried, and a user plane, where media information is transmitted (audio, video, etc.). Next figure illustrates this graphically (AAA protocols are excluded in this figure; Diameter will be treated in Annex F in that regard).

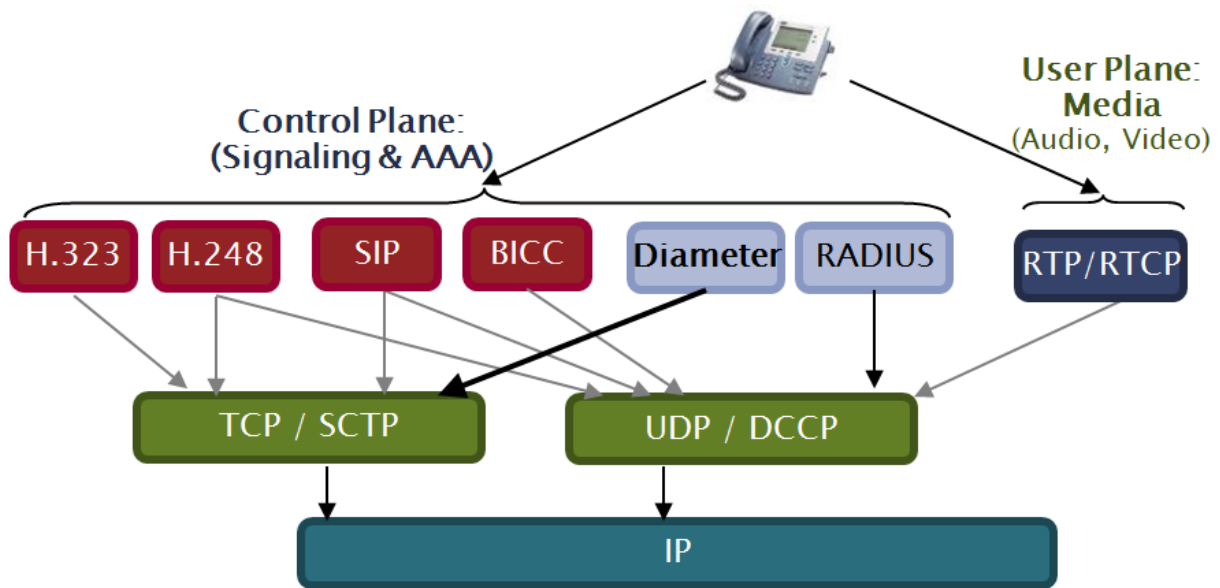


Figure E - 6. Control and User planes in VoIP.

Protocols acronyms exhibited in the previous figure are briefly described in following sections of this annex.

#### E.4.1 VoIP Control Plane Protocols

Following are described the communication protocols used in the control plane of an IP network, either for VoIP as for other means like AAA (Authentication, Authorization and Accounting). All protocols will be briefly described, for later focusing on the most crucial ones for the IMS and LTE, i.e. SIP and Diameter (the latter will be approached in next chapter)

- Bearer Independent Call Control (**BICC**): Specified by ITU-T Q.1901, it comprises ISUP evolution as it splits the user plane from the control plane (signaling). Therefore, signaling information may traverse different nodes of either the user plane. Besides, it may be conveyed either through SS7 and IP networks.
- **H.323**: Multimedia communication packet based system protocol specified by ITU-T (ITU-T Recommendation H.323). Unlike BICC, it was specified from the

beginning for IP networks. In H.323, information from either user or control planes do not need to go through the same nodes.

- **Session Initiation Protocol (SIP)**: Specified by IETF RFC 3261 for the establishment and management of multimedia session through IP networks. Chosen by 3GPP as the session control protocol for the IMS and LTE (where VoIP is renamed as VoLTE). It inherits HTTP and SMTP characteristics. It has big advantages compared to BICC and H.323, namely:
  - For being text-based, it's easier to debug, extend and use for service creation.
  - It does not differentiate «User-to-Network Interface» (UNI) from « Network-to-Network Interface» (NNI).
- **Media Gateway Control Protocol (MGCP)**: Specified by IETF RFC 2805. It comprises the combination of SGCP (*Simple Gateway Control Protocol*) and IDPC (Internet Device Control Protocol).
- **MEGACO (H.248)**: Media Gateway Control Protocol specified by ITU-T Recommendation H.248. It combines MGCP and MDCP (*Media Device Control Protocol*). Initially specified by IETF (RFC 3525) obsoleted by IETF RFC 5125. It comprises a master/slave type of protocol. It splits the control and media processing call logics through a gateway.
- **Remote Authentication Dial In User Service (RADIUS)**. Application layer protocol specified by IETF RFC 2865. Client/server type protocol, uses UDP as transport. Originally used by ISP's to manage Internet access when the user carried out the dial-up (modem connection via the telephone line) or by organizations for providing access to fixed/wireless networks to integrated email services.
- **Diameter**: RADIUS evolution specified by IETF RFC 3588 (currently obsoleted by IETF RFC 6733). It consists of a base protocol extended by self-nominated «Diameter extensions», which constitute adaptations or extensions to Diameter in order to fit specific applications within a particular environment. Modern IP-

based networks like the IMS or LTE use Diameter in a wide variety of interfaces, even though not all of them use the same Diameter application. For example, the IMS defined a Diameter application together with SIP during session establishment, as well as another way to manage accounting for subscriber credit control.

#### **E.4.1.1 Session Initiation Protocol (SIP)**

This section exposes a brief description of SIP protocol functionality as described in IETF RFC 3261 (2002, SIP «version 2.0»). Likewise, concepts introduced by 3GPP TS 24.229 (version 3) will be mentioned for call control based on SIP and SDP.

Inspired by HTTP (Hyper Text Transfer Protocol), SIP has become the preferred standard for controlling multimedia communications over IP, exceeding previous preference to protocols such as ITU-T's H. 323, H. 245 or H. 225. Reasons for this reside on several competitive advantages, namely:

- ✓ Text coding (format based on HTTP).
- ✓ Easy to code.
- ✓ Uses primitives (messages).
- ✓ End-to-end signaling.
- ✓ General purpose protocol: not limited to telephony. It can be used for a wider variety of multimedia communications and services such as authentication, location, call control, etc.
- ✓ Provides presence and mobility.
- ✓ By design, SIP is independent of access technology.
- ✓ Flexible and extensible. SIP messages may transport an arbitrary payload (SDP, IM, JPEG, any MIME type, etc.).
- ✓ Multiple enhancements are defined for SIP, each one comprising a specific RFC. SIP embraces a compatibility mechanism which allows the addition of new capabilities without producing any impact in those operating systems which do not support the new capability.
- ✓ Supports five facets for establishing and releasing multimedia communications.

- User location: determination of the final endpoint to use for the communication.
- User availability: determination of the calling party to be part of the requested communication.
- User capabilities: determination of which media and media parameters to use within the communication.
- Session configuration: establishment of session parameters between ends (calling and called party).
- Session management: includes session transfer and release, live call modification and service invocation.

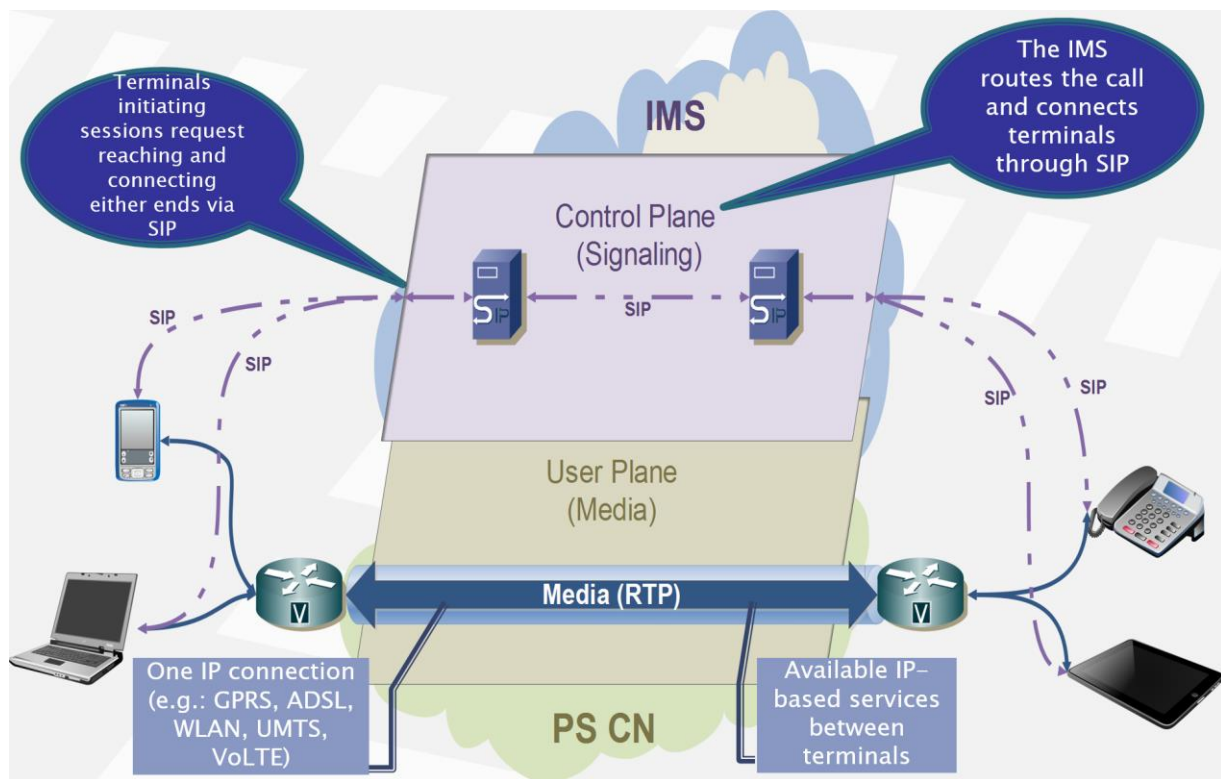


Figure E - 7. Basic call control via SIP over IP networks overview.

SIP then comprises a control plane protocol enabled for establishing, modifying and releasing multimedia sessions such as telephone or conference calls via the Internet (indistinctly if over IPv4 or IPv6). SIP can also invite new participant or SIP User Agents (SIP UA) to already established multicast sessions. It can also remove or add media over an existent multimedia session. Likewise, it supports mapping of



name and redirect services in a transparent way, which embraces personal mobility (i.e. users can maintain an extrinsic visible identifier regardless of their network location).

#### E.4.1.1.1 SIP Architecture and Agents

This section describes SIP architecture components and agents.

A SIP User Agent (**UA**) comprises a logic entity for origin (Client) or termination (Server) of a SIP transaction. A UA can act as client or server but can only assume one of those roles during a SIP transaction. A user agent is available in devices (adaptors, SIP phones, etc.) and applications (Softphones).



Figure E - 8. Examples of SIP User Agents.

So, a UA is divided in the following types:

- User Agent Client (**UAC**): logical entity of a SIP transaction by means of a request creation and use of a transactional SIP state machine for submission. The duration of a SIP transaction determines the time interval of the role of an agent as UAC. In case of receiving a request after completion of a transaction, the same agent role changes to UAS for processing the new SIP transaction.

- User Agent Server (**UAS**): logical entity that generates a response to a SIP request. The response accepts, rejects or redirects the request. The duration of a SIP transaction determines the time interval of the role of an agent as UAS. In case of creating a request after completion of a transaction, the same agent role changes to UAC for processing the new SIP transaction.
- Back to Back User Agent (**B2BUA**): logical entity that receives a request and processes it as a user agent server (UAS). In order to determine how the request should be answered, it acts as a user agent client (UAC) and generates requests. Unlike a proxy server, it maintains dialog state and must participate in all requests sent on the dialogs it has established. Since it is a concatenation of a UAC and UAS, no explicit definitions are needed for its behavior.

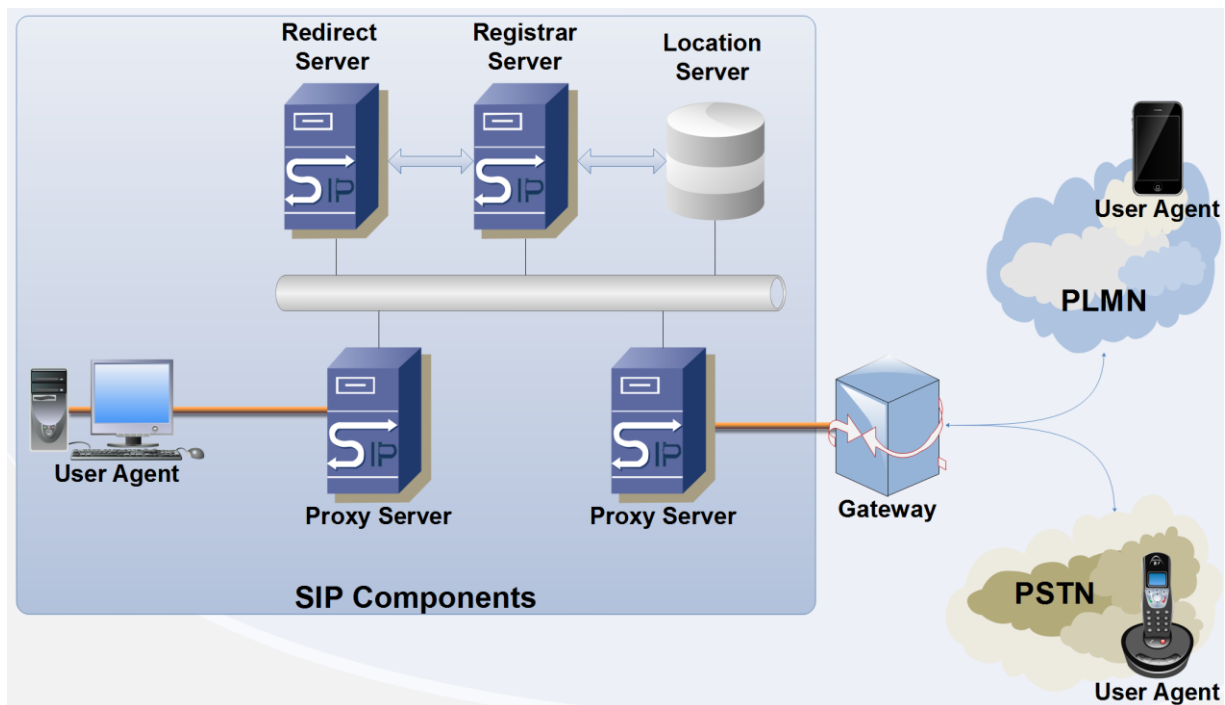


Figure E - 9. SIP Architecture components and agents.

SIP architecture servers are described next.

- **Proxy Server:** intermediate entity that acts as both server and client for the purpose of making requests on behalf of other clients (i.e. acts as UAC and UAS on behalf of other clients). Its main purpose is routing requests so as they are properly directed to the destination's closest entity.

Proxy Servers ensure policies (e.g. user authorization for call establishment).

Proxy Servers also interpret and if case of being necessary, rewrites specific parts of a request message before forwarding.

- **Redirect Server:** intermediate entity acting as UAS to reroute calls to external domains servers. It generates code 3xx responses to indicate the source (UAC) to contact an alternative address set or URI (Universal Resource Identifier).
- **Registrar Server:** intermediate entity acting as UAS for user registration administration. It is located either in Proxy or Redirect servers. It accepts SIP REGISTER requests and locates the received information in the adequate location server according to the domain/realm it handles.
- **Location Server:** intermediate entity acting as UAS for managing the association between logical and physical SIP addresses. Usually located in a Registrar. A location service is used for obtaining information of the possible locations of the called party. The bindings may be created and removed by multiple ways (RFC 3261 defines a REGISTER method for binding's update).

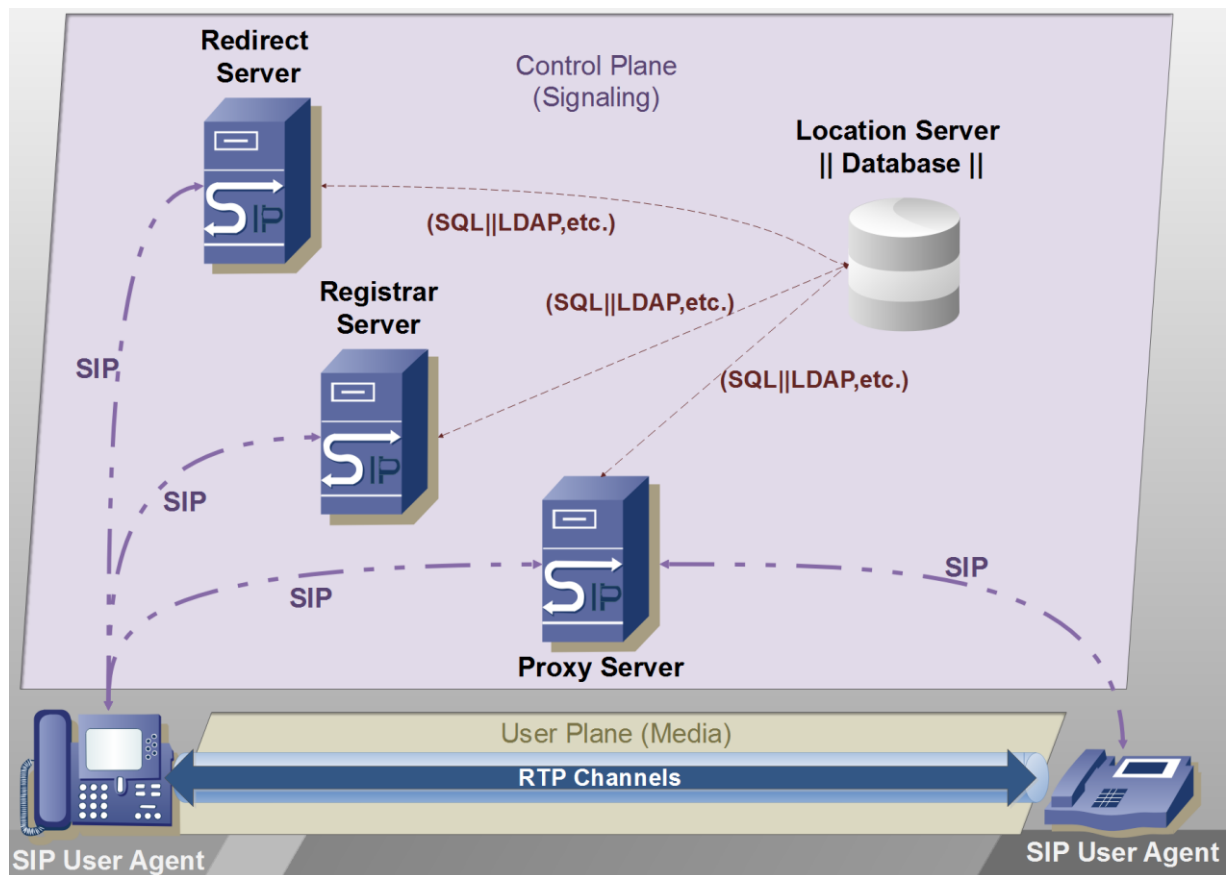


Figure E - 10. SIP Servers involved in multimedia communications controlled by SIP.

#### E.4.1.1.2 SIP Transactions and User Agents roles

The establishment of a SIP session is carried forward from a set of SIP proxies. The communication path for multimedia session is defined during the establishment of the SIP session. However, user multimedia data transfer is not conveyed yet. Once the SIP session is established, normally a smaller number of SIP proxies is kept for the rest of the session that during its establishment. Thereafter, transfer of multimedia information between user agents can begin.

The relationship between the SIP and media session remains during the entire session in either planes. The multimedia session in the user plane remains under the control of SIP. Any change in the definition multimedia session, as its termination, is signaled between user agents via SIP.

The figure below shows the establishment of a multimedia session via SIP signaling between two SIP user agents, called «UA1» and «UA2».

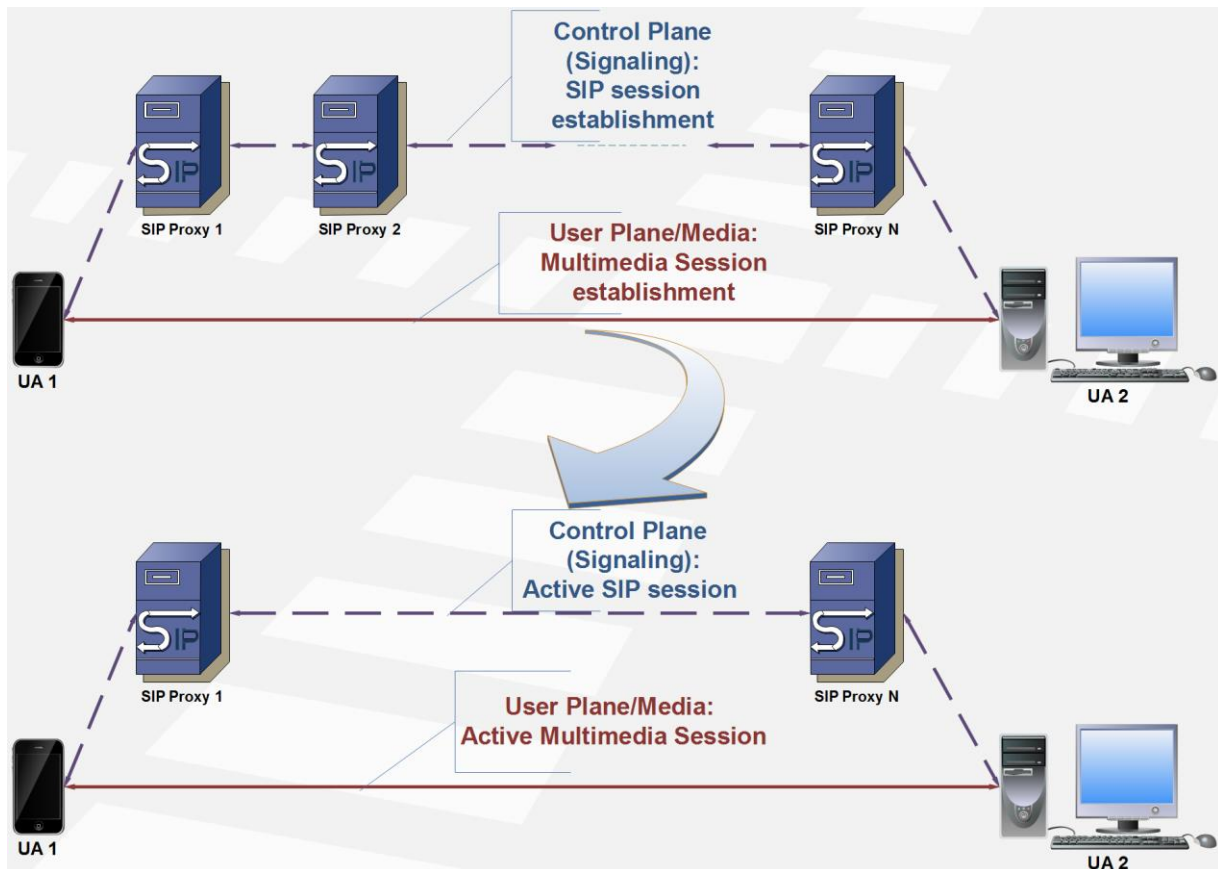


Figure E - 11. SIP trapezoid.

A SIP transaction coexists in the client-server transaction state model. The user agent initiator of the transaction acquires the role of client or «UAC», as the user agent that receives and executes the transaction acquires the role server or «UAS»

In the case of an INVITE transaction, some of the elements contained in the request message and provisional responses have the purpose of keeping the SIP session active after the INVITE transaction satisfactory completion. In other words, they won't be needed during the context of the current transaction, but will be used in subsequent ones within the established SIP session.

The execution of a transaction between two UAs attempts the establishment of a SIP session between these two user agents depending on the type of executed transaction at that moment and its result. For example, the execution must distinguish the context of REGISTER from INVITE transactions, while the former does not derive in the establishment of SIP session, the latter has the capability of creating it outside of the context of a pre-existent session.

The execution of an INVITE transaction could include the sending of an ACK request. This will be the case when the final response to the INVITE request is part of a failed transaction. Then, ACK message becomes part of the INVITE transaction. In case the INVITE transaction success, an ACK message will also be sent after INVITE transaction conclusion. The difference in this case resides in the fact that the ACK request constitutes a separated SIP transaction, without the need of a final or transitory responses. Next figure portrays these two scenarios.

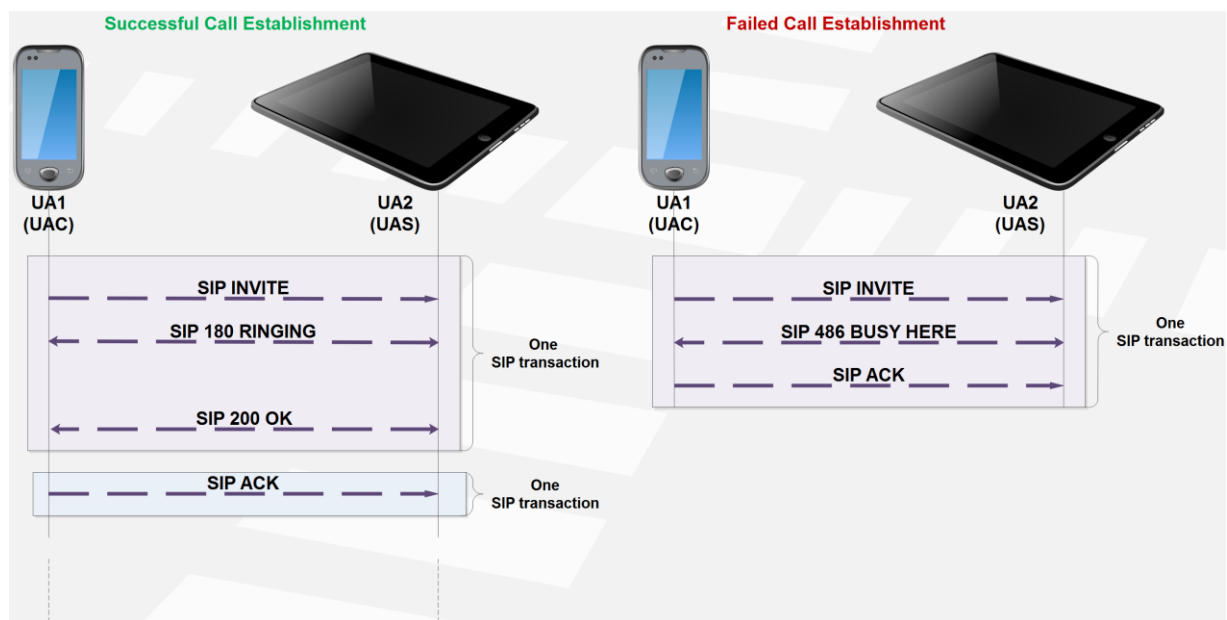


Figure E - 12. SIP call establishment transaction scenarios.

The left side of the previous call flow diagram shows a satisfactory call establishment. Response codes 180 or 200, as well as associated labels as «Ringing» or «OK» are part of the SIP message «Status Line». When UA1 has received the final satisfactory response «200 OK», the SIP session between UA1 and UA2 user agents has been established. UA1 then initiates a new transaction with SIP

«ACK» request towards UA2, so as to confirming that the previous transaction has been properly handled. Similarly, the right side of the previous call flow diagram displays the case of a failed call establishment. After the reception at UA1 of final unsatisfactory «486 Busy Here» response message from UA2, a session is not established. Then, UA1 sends a SIP «ACK» request to UA2 for confirming the reception of the transaction ending message. Contrarily to the previous scenario, ACK message derived from the unsatisfactory response is included in the same SIP transaction (INVITE), as explained before.

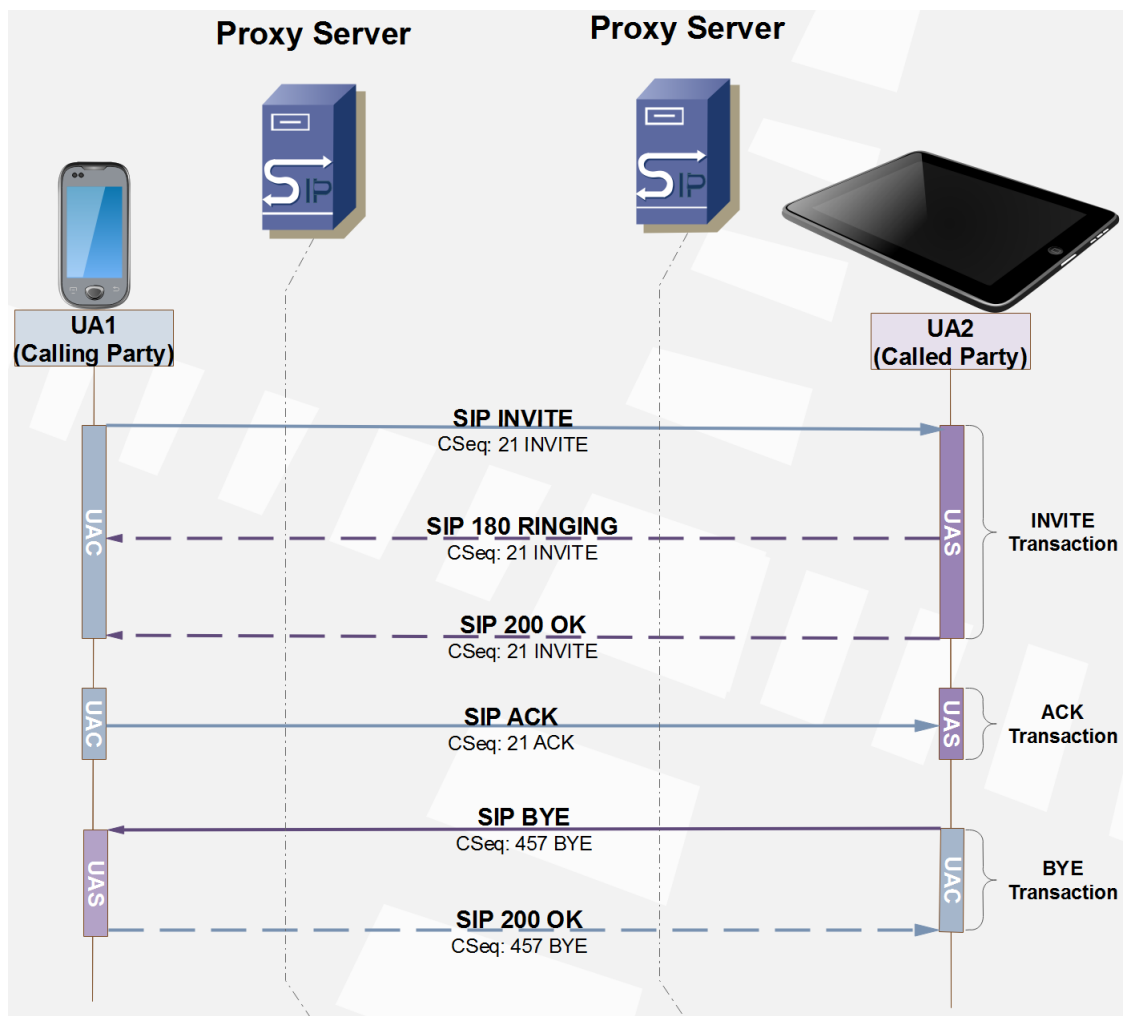


Figure E - 13. Example of SIP UA roles during SIP session transactions.

A classical conceptual error encompasses the association of UAC and UAS with a node or entity, e.g. a SIP phone. A SIP phone establishing a call (SIP session)

is frequently wrongly considered as the whole session UAC. As mentioned before, UAC and UAS are roles an UA may hold during a SIP session, depending if the UA is the initiator or receiver of a transaction request. This fact explained is graphically displayed in the previous call flow diagram example containing SIP INVITE, ACK and BYE transaction, in which the SIP header «Cseq» parameter identifying each transaction is shown. Cseq parameter will be explained in next sections of this document.

A SIP transaction instance constitutes a process that might be created by a user agent. The UA creates the request message, then the corresponding client transaction state model instance begins and passes the request message so it then handles the transaction towards the final end. A similar transaction between the user agent and the transaction instance occurs at the receiving end.

The layer above the transaction layer is called the transaction user (TU). Each of the SIP entities, except a stateless proxy, is a transaction user. When a TU wishes to send a request, it creates a client transaction instance and passes the request along with the destination IP address, port, and transport to which to send the request. A TU that creates a client transaction can also cancel it. When a client cancels a transaction, it requests the server to stop further processing, revert to the state that existed before the transaction was initiated, and generate a specific error response to that transaction. This is done with a CANCEL request, which constitutes its own transaction, but references the transaction to be cancelled.

Next diagram shows a graphical representation of an INVITE transaction between two UAs. The mentioned timers in both state models are used to rule the transactional signaling (e.g. to trigger a retransmission). These timers are described in SIP specification, from where the next diagram was extracted (i.e. IETF RFC 3261).



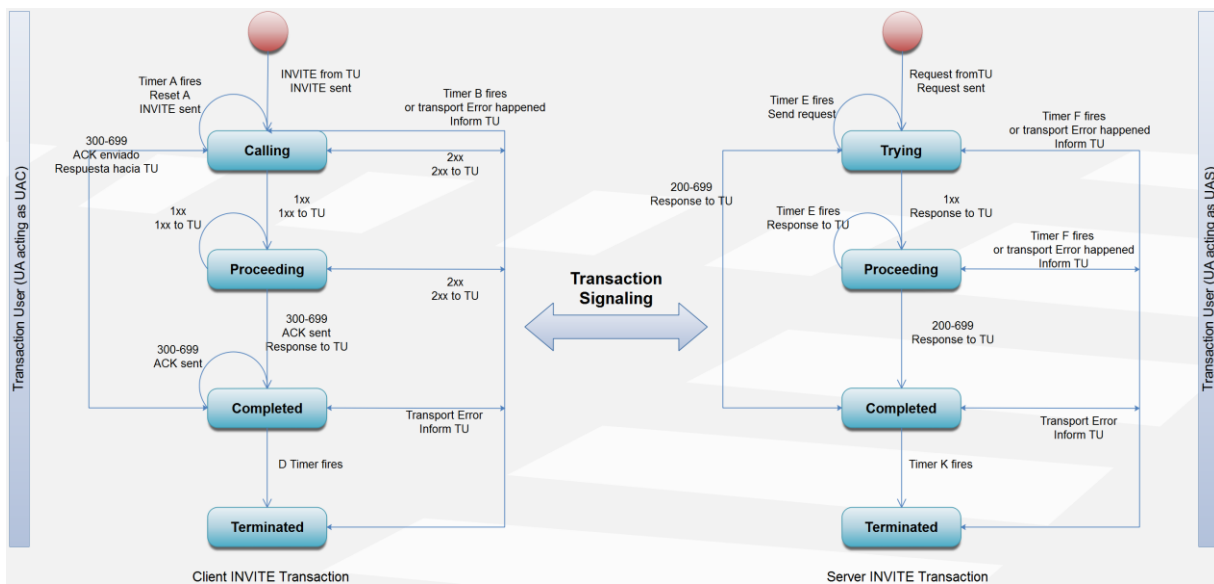


Figure E - 14. SIP INVITE Client/Server transaction state models.

SIP discriminates between the next four transaction state models

1. Client INVITE Transaction
2. Server INVITE Transaction
3. Client Non-INVITE Transaction
4. Server Non-INVITE Transaction

If successful, the INVITE transaction derives in the establishment of a SIP session between corresponding user agents (note: a SUBSCRIBE transaction might also derive in a SIP session establishment). The following communication between these two user agents (e.g. to recognize the successful execution of the INVITE transaction, or request a SIP session termination), is carried out between these two user agents.

When the INVITE transaction is not successful, there is no established SIP session between corresponding user agents. In fact, an intermediary proxy could have generated the final response (e.g. «500 Server Internal Error»). Therefore, in case an INVITE transaction is not satisfactory, the ACK message is used for final reception recognition, a response different than 2xx is sent as part of the transaction. The ACK message traverses the same chain of SIP proxies that the SIP INVITE

message crossed. The corresponding SIP proxies, as the UAS for this request, destroys the transaction process at the moment of receiving the ACK message.

The reason for discriminating between the client and server transaction states resides in the fact that a UAC might retransmit the request message when it hasn't received a provisional response for that request. The retransmission might be repeated according to a defined pattern. For the UAS, the retransmission might apply for the final response.

The previous description of the differentiated use of the ACK message is also reflected as for the UAC or UAS state model. A Client INVITE transaction model possesses the capability of ACK message submission, while the Server INVITE transaction model possesses the capability of ACK message reception.

#### **E.4.1.1.3 SIP in the IMS**

SIP constitutes one of the protocols to be used in order to build a complete multimedia architecture. Among these other protocols are the following:

- Session Description Protocol (**SDP**, IETF RFC 4566) for description of multimedia sessions. SDP covers functionalities such as session invitation, announcement and parameter negotiation. SDP is not responsible for content delivery but for establishing a negotiation between the session stakeholders through parameters such as type of content, format and all those parameters associated with this type of negotiation purpose. This set of parameters compose the session profile.
- Media Gateway Control Protocol or MEGACO (ITU-T **H.248**) for the control of PSTN Gateways.
- Real-time Transport Protocol y Real-time Transport Control Protocol (**RTP/RTCP** as for IETF RFC 3550) for the transport of multimedia information (audio/video) in real time and QoS (Quality of Service) feedback.

- Real-time Streaming Protocol (**RTSP**, IETF RFC 2326) for the control of transmitted media delivered.
- **Diameter** (IETF RFC 6733) for AAA (Authentication, Authorization and Accounting) functions and extensions (Diameter will be further explained in annex F).

For providing a complete set of services, SIP must be used together with these protocols, either in the signaling plane (to which it belongs along with SDP, Diameter and H.248) or the user plane (RTP/RTCP or RTSP). However, SIP's basic functionalities does not depend on none of these protocols. Instead, SIP provides primitives that can be used to implement different services. Hence, SIP is completely independent of the object it is transporting. These objects might constitute session descriptions written in different formats (typically through SDP) or any type of information (e.g. for IM -Instant Messaging-).

SIP does not prescribe how a conference should be managed. It can be used to log on using another conference control protocol. Since SIP messages and the sessions set by it can go through completely different networks, SIP does not and is not able to establish any kind of network resource reservation.

The nature of the services provided makes security an important topic. To that end, SIP provides a suite of security services that include denial of service, authentication (for either user-to-user and proxy-to-user), integrity protection, encryption and privacy services.

SIP constitutes the call control protocol for use in UMTS' IMS and is used in the following interfaces of such network subsystem:

- UE (User Equipment) <-> CSCF (Call Session Control Function);
- Interfaces among different CSCFs;
- CSCF <-> AS (Application Server);
- CSCF <-> ISC Gateway Function;
- ISC Gateway Function <-> AS;
- CSCF <-> MGCF (Media Gateway Control Function);

- S-CSCF (Serving CSCF) <-> MRFC (Multimedia Resource Function Controller);
- AS <-> MRFC;
- S-CSCF <-> MRB (Media Resource Broker);
- AS <-> MRB;
- MRFC <-> MRB;
- CSCF <-> BGCF (Breakout Gateway Control Function);
- BGCF <-> MGCF;
- CSCF <-> IBCF (Interconnection Border Control Function);
- IBCF <-> AS;
- IBCF <-> MRFC;
- IBCF <-> MRB;
- E-CSCF (Emergency CSCF) <-> LRF (Location Retrieval Function);
- Interfaces among different BGCFs;
- CSCF <-> IMS externa;
- E-CSCF <-> EATF (Emergency Access Transfer Function);
- P-CSCF <-> ATCF (Access Transfer Control Function);
- I-CSCF <-> ATCF;
- ATCF <-> IBCF.

#### E.4.1.1.4 SIP Addresses

SIP addresses are known as SIP URI (SIP Uniform Resource Identifier) and they identify a communication resource, for example:

- ✓ An online user.
- ✓ A multi-line telephone appearance.
- ✓ An email account within a messaging service.
- ✓ A PSTN telephone number in a Gateway.
- ✓ A group within an organization (sales department, support, etc.).

SIP URI's adopt the following general format (whose basic example would be: `sip:user@host.domain`):

`sip:user:password@host:port;uri-parameters?headers`

More examples are displayed next (Other kind of URL is allowed, i.e. http, mailto, etc.):

<sip:user24@sip.mydomain.com>

<sip:alice@atlanta.com;maddr=239.255.255.1;ttl=15>

<sip:voicemail@iptel.org?subject=callmecarol@ws.domain2.com;transport=tcp>

[sip:sales@hotel.xy; geo.position:=48.54091\\_-123.84120](sip:sales@hotel.xy; geo.position:=48.54091_-123.84120)

Users can be additionally identified via SIPS URI (SIP SECURED URI), e.g. <sips:alice.smith@domain.com>. Entities contacting SIPS URI use TLS (Transport Layer Security) protocol between the UAC and the domain to which the URI belongs. From there, the specific security mechanism depends on the realm's policies. Any resource described by a SIP URI can be updated to SIPS URI through a simple scheme modification in case it is needed to establish a secure communication.

It is possible to include a telephone number within a SIP URI by using the format exposed in the following example:

<sip:+1-212-555-0293@operator.com;user=phone>

This format is needed given the fact that SIP requires that the registered URI keeps being a SIP URI, as it is not possible to register a TEL URI -public identity format used in the IMS for connecting an IMS terminal with a PSTN telephone-, but it is possible to register a SIP URI containing a telephone number as in the preceding example.

#### **E.4.1.1.5 SIP Messages**

SIP messages are based on HTTP (HyperText Transfer Protocol) thus it is a textual request-response protocol, using the set of characters ISO 10646 coded in UTF-8. It also uses MIME (*Multipurpose Internet Mail Extensions*, defined by IETF RFC 2045). MIME allows sending several attached files of different formats such as JPEG images, MPEG videos, emails, etc. SIP uses TCP, SCTP or UDP as transport protocol. Lines must end with CRLF (Carriage Return -ASCII 13, \r- Line Feed -ASCII 10, \n-).

A client user agent (UAC) send requests which are responded by a server user agent (UAS). As explained earlier, a SIP transaction consist of a request sent from a UAC, zero or more provisional responses and a final response from the UAS.

The structure of a SIP message is composed by a «Start Line» for a message request or a «, followed by a variable amount of «Header Fields» (six of them are always mandatory), followed by an «Empty Line» and finally the message «Body», as depicted next:

```
Start Line || Status Line
Header Fields
Empty Line
Body
```

Following figures display examples of request and response messages and their structures.

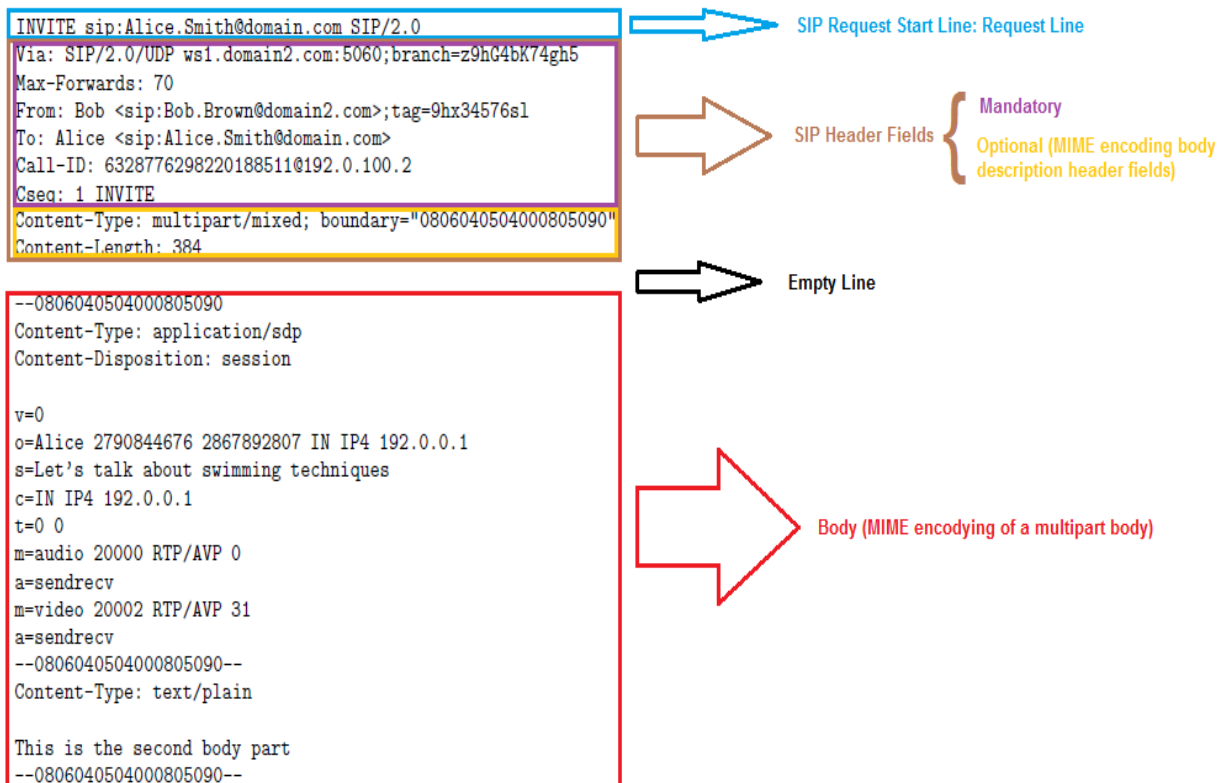


Figure E - 15. SIP request message structure example.

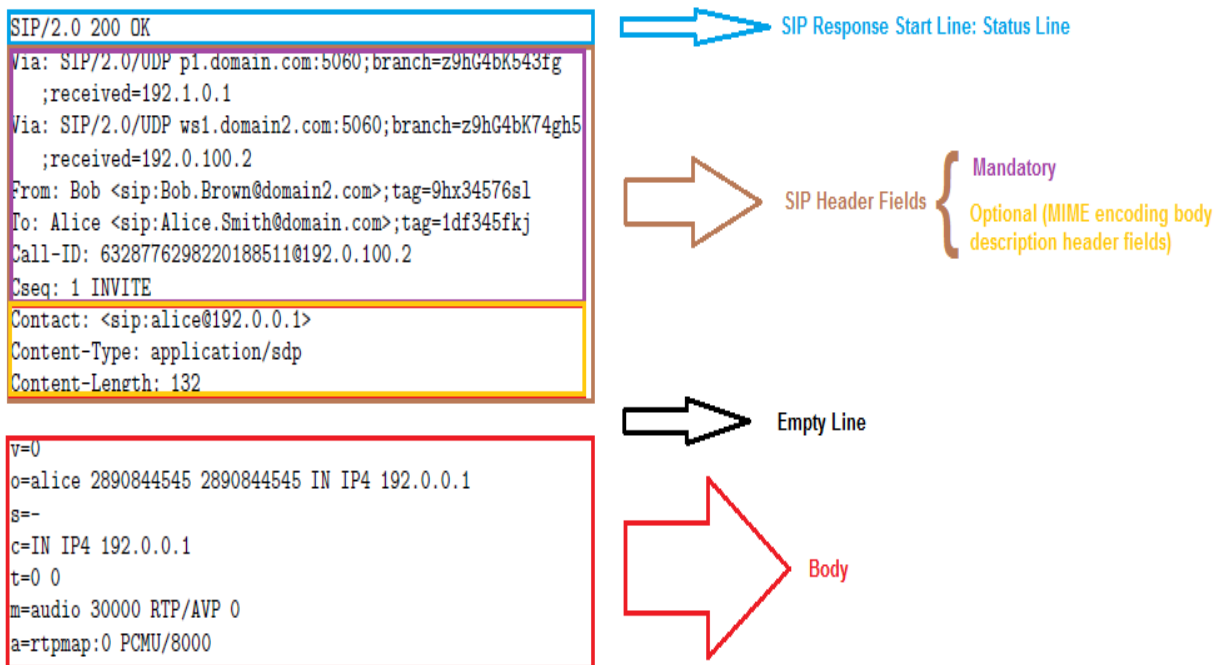


Figure E - 16. SIP response message structure example.

In multimedia sessions over the Internet the session establishing information must contain enough essential information to deliver to the end peer to join the session such as the IP address and port (socket) by which the media flow must be conveyed, as well as the Codecs used for coding media. The most common format for describing multimedia sessions is the one established by SDP (Session Description Protocol), specified by IETF RFC 2327, which comprises a textual format for multimedia session description.

SDP consists of two sections: 1) session information, 2) media information.

SIP is independent of SDP (even though it's the most used, it is not the only session description format used by it; e.g. SDP is not used for IM or USSD over IMS or USSI).

SDP is contained in the SIP body. Following, an example of SDP:

```

v=0
o=Alice 3239874567 4447990887 IN IP4 10.0.0.1

```

```

s=Let's talk about us
c=IN IP4 10.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0
a=sendrecv
m=video 20002 RTP/AVP 31
a=sendrecv

```

The previous SDP example contains the session description initiated by the user «Alice», whose IP address is 10.0.0.1. The port numbers where it is expecting to transmit audio and video in duplex mode are 20000 and 20002, through RTP/AVP, and the audio/video codecs supported are placed as «0» (ITU-T G.711 according to  $\mu$  law) and «31» (ITU-T H.261). The subject of the conversation is «Let's talk about us».

The following table lists the acronyms SDP types and their meanings.

Type	Meaning	Type	Meaning
v	Protocol version.	u	URL containing the session description.
b	Bandwidth info.	t	Time at which the session activates.
o	Session owner.	e	Email address from where to obtain information of the session.
z	Time zone.	t	Time at which the session repeats.
s	Subject of the session.	p	Telephone number from where to obtain information of the session.
k	Encrypting key.	m	Media line.
i	Information about the session.	c	Information about the connection.
a	Attributes line.	i	Information about the media line.

Table E - 1. SDP acronyms types and meanings.



SIP messages can traverse communication paths in two ways: end-to-end or hop-by-hop. Next figure shows this concept graphically.

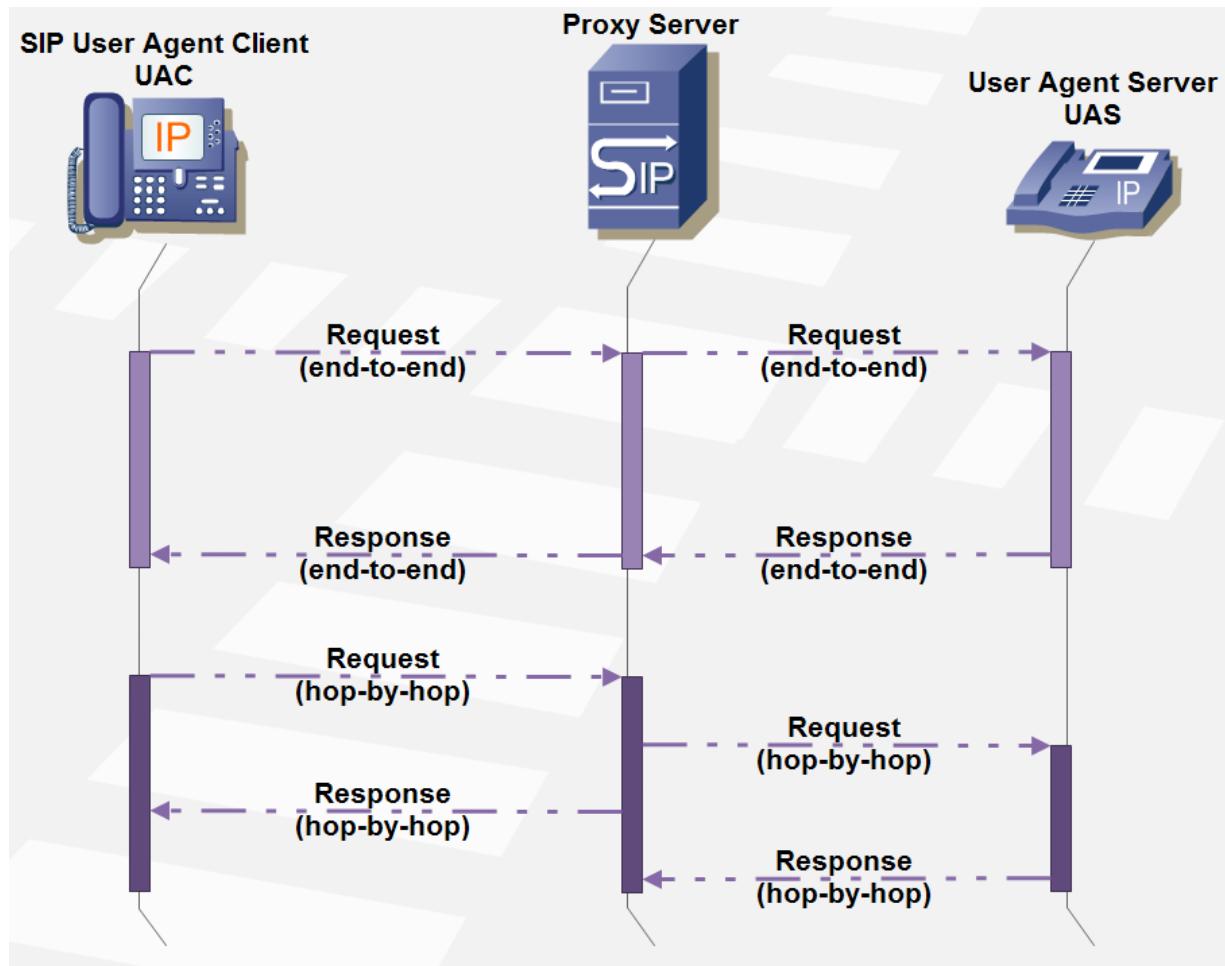


Figure E - 17. SIP end-to-end versus hop-by-hop messages.

The «Request Line» from a SIP Request message is composed of the following:

- ✓ Method name
- ✓ *Request URI*
- ✓ Protocol version.

An example of a SIP «Request Line» is as follows:

```
INVITE sip:Alice.Smith@domain.com SIP/2.0
```

SIP methods are briefly described in the following table.

SIP method name	Meaning
ACK	<ul style="list-style-type: none"> <li>• Acknowledges final response for an INVITE (other SIP methods do not use this backward feedback procedure).</li> <li>• The UAS identifies to which INVITE the ACK corresponds through the Cseq number (thus, it is not increased in an ACK).</li> <li>• In a scenario where the media are not recognized after an INVITE, the ACK might contain a message body of type <i>application/sdp</i>.</li> <li>• In 2xx responses, ACK is end-to-end, otherwise it is hop-by-hop when stateful proxies exist in the path (a hop-by-hop ACK reuses the same Branch ID given it is considered as part of the same transaction; an end-to-end ACK uses a different Branch ID as it is considered as part of another transaction).</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards.</li> </ul>
BYE	<ul style="list-style-type: none"> <li>• Ends an established session (it is considered established whenever it received a response with 2xx range code or an ACK has been sent).</li> <li>• It is sent by UAs participating of a session, never by proxies or third parties.</li> <li>• It's an end-to-end method.</li> <li>• A UA responds a BYE with response code <i>481 Dialog/Transaction Does Not Exist</i> when the dialog is unknown.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards.</li> </ul>
CANCEL	<ul style="list-style-type: none"> <li>• It cancels a pending request (ends a call/session that has yet not been confirmed, e.g. method used by an UA to cancel an INVITE previously sent that has not yet received an ACK).</li> <li>• It is a hop-by-hop request and receives a stateful response of the next element.</li> <li>• A UA responds with <i>200 OK</i> to the CANCEL and <i>487 Request Terminated</i> to the INVITE.</li> <li>• A proxy resends a CANCEL to the next elements with pending requests from the previous INVITE.</li> </ul>

	<ul style="list-style-type: none"> <li>• If a final response was previously received (messages crossing), the UA shall terminate the session with a BYE.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards.</li> </ul>
INFO	<ul style="list-style-type: none"> <li>• Call monitoring. It transports signaling information of the telephone network (e.g. ISUP within the message body) between two UAs that have established a media session.</li> <li>• Every INFO request will receive a <i>481 Transaction/Dialog Does Not Exist</i> for unknown dialogs.</li> <li>• This method always increments the Cseq number.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards.</li> </ul>
INVITE	<ul style="list-style-type: none"> <li>• Establishes a session (e.g. user agent call, call transfer, etc.).</li> <li>• INVITE responses are always acknowledged with an ACK.</li> <li>• They usually contain a body encompassing the media information of the calling party (if not, it is included in the ACK response for evaluation, if not acceptable, the calling party shall end the session through a BYE).</li> <li>• A media session is established when messages INVITE, 200 OK and ACK have been exchanged between UAC and UAS, which establishes a dialog among them.</li> <li>• The UAC sending the INVITE establishes a unique global identifier that identifies the call during its extension through the <i>Call-ID</i> header field.</li> <li>• The Cseq is increased for each new request for the same <i>Call-ID</i>.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Contact, Max-Forwards.</li> </ul>
NOTIFY	<ul style="list-style-type: none"> <li>• Notifies the user agent about its capabilities (e.g. online/offline status of an instant messaging/presence service).</li> <li>• It is always sent within a dialog.</li> <li>• It usually receives 200 OK. If it receives <i>481 Dialog/Transaction Does Not Exist</i>, the transaction automatically is terminated and no further NOTIFY messages are sent.</li> <li>• A NOTIFY is always sent at the beginning and end of a subscription.</li> <li>• The header field «Event» indicates the packet name</li> </ul>

	<p>used in the subscription, while the header field «Subscription-State» indicates its current state.</p> <ul style="list-style-type: none"> <li>• Mandatory header fields: To, Via, To, From, Call-ID, Cseq, Max-Forwards, Event, Allow-Events, Subscription-State.</li> </ul>
OPTIONS	<ul style="list-style-type: none"> <li>• Requests information to a UA or server about its capabilities (e.g. supported messages and codecs).</li> <li>• A 2xx response code might contain the header fields <i>Allow</i>, <i>Accept</i>, <i>Accept-Encoding</i>, <i>Accept-Language</i> y <i>Supported</i> indicating the capabilities.</li> <li>• Tags such as <i>audio</i>, <i>video</i> o <i>isfocus</i> should be included in the header field <i>Contact</i>.</li> <li>• It is never sent by a proxy (albeit the request could be destined to it)</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards.</li> </ul>
PRACK	<ul style="list-style-type: none"> <li>• Recognizes the reception of a provisional response (code 1xx) of reliable transport.</li> <li>• Does not apply to the reception of non-reliable transport provisional response (code 100 Tying).</li> <li>• It is generated by a UAC when a provisional response has been received containing a reliable sequence number (header field <i>RSeq</i>). PRACK echoes this number as well as the Cseq of the response within the header field <i>RAck</i>.</li> <li>• If a PRACK is not received during a determined time, the message is retransmitted. The reception of a PRACK confirms the delivery of the response and stops subsequent retransmissions.</li> <li>• The combination of Call-ID, Cseq and Rack allows the UAC to correlate the PRACK with the provisional response it is acknowledging.</li> <li>• PRACK always increases the Cseq number.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards, Rack.</li> </ul>
PUBLISH	<ul style="list-style-type: none"> <li>• Used by a UA to send event status information to a server known as ESC (Event State Compositor).</li> <li>• After a PUBLISH, the ESC generates NOTIFY to «watching» elements.</li> <li>• Opposed to NOTIFY, PUBLISH is not sent within a SIP dialog.</li> <li>• 200 OK response contains information of the event generated by the ESC, information that is contained in the header field <i>SIP-ETag</i>. This information might be</li> </ul>

	<p>used to update the published information.</p> <ul style="list-style-type: none"> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards, Contact, Event, Allow-Events, Expires, Min-Expires</li> </ul>
REGISTER	<ul style="list-style-type: none"> <li>• It maps a public URI with the user's current location.</li> <li>• Delivers a contact address and an alias to the Registrar. For example: <code>sip:UAA@example.com</code> is an alias for <code>sip:UserA@10.20.30.40</code>. The Registrar <code>example.com</code> might redirect the calls for <code>UAA</code> towards the address <code>10.20.30.40</code>.</li> <li>• A UA needs this message for receiving calls.</li> <li>• A UA might receive responses with code 3xx (redirection) or 4xx (failure) containing the header field <i>Contact</i> with the location of the proper Registrar.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards.</li> </ul>
SUBSCRIBE	<ul style="list-style-type: none"> <li>• Requests to be notified about a particular event through a NOTIFY method.</li> <li>• A successful subscription establishes a dialog between UAs.</li> <li>• The header field <i>Expires</i> indicates the duration of the subscription (which might be refreshed via another SUBSCRIBE).</li> <li>• A UAC must be prepared to receive NOTIFY messages (from possible different UAS) previous to the unique possible final 200 OK response.</li> <li>• The type of subscription event is established in the <i>Event</i> mandatory header field.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards, Contact, Event, Allow-Events.</li> </ul>
UPDATE	<ul style="list-style-type: none"> <li>• Modifies the state of a session without changing the SIP dialog state.</li> <li>• None of the parts involved in a session may reinvite another one within a pending session (INVITE sent but without a received response): for this case UPDATE method is used.</li> <li>• UPDATE uses include putting a call on hold, renegotiate QoS or other end-to-end status attributes negotiation previous to the establishment of the session.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards, Contact.</li> </ul>
	<ul style="list-style-type: none"> <li>• Used to transport an instant message (IM) through SIP.</li> <li>• They do not need a dialog to be sent, as well as they do</li> </ul>

MESSAGE	<p>not establish a SIP dialog by themselves.</p> <ul style="list-style-type: none"> <li>• The content of the message is sent in the body of the message as a MIME attachment.</li> <li>• It is mandatory for a UA to support the <i>plain/text</i> format for this method (others like <i>text/html</i> or <i>message/cpim</i> could be supported).</li> <li>• A response message within a conversation is not sent within a 200 OK message but within another SIP MESSAGE.</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards.</li> </ul>
REFER	<ul style="list-style-type: none"> <li>• Instructs a UA to send an Access request to a URI or URL identified in the header field <i>Refer-To</i>.</li> <li>• Very used for transferring calls (when URI is sip or sips) or obtaining a Web page.</li> <li>• Might be used inside or outside a SIP dialog.</li> <li>• It does not use the INVITE state machine (the UAS responds with 202 Accepted without waiting the sent request to be completed).</li> <li>• Mandatory header fields: Via, To, From, Call-ID, Cseq, Max-Forwards, Refer-To.</li> </ul>

Table E - 2. SIP Methods main characteristics.

A «Status Line» of a SIP response message is composed of the following:

- ✓ Protocol version (currently SIP/2.0).
- ✓ «Status Code» of the transaction in numeric format. Following tables briefly described the transaction status code ranges and their meanings.
- ✓ Status of the transaction in human legible format.

An example of a SIP «Response Line» is as follows:

#### SIP/2.0 401 Unauthorized

Status code range	Meaning
100-199	<p>Provisional or informative result.</p> <p>The UAS informs the UAC about the progress of a transaction request. The provisional response might include additional information required by the UAC for transaction resume.</p>

200-299	<p>Successful request result. The transaction has been executed successfully.</p>
300-399	<p>Redirected request. This class of response informs the UAC that the indicated destination within the request message should be contacted in an alternative way or that an alternative service should be requested from the destination.</p>
400-499	<p>Request failure. The UA receiver of this request, in its UAS role, has indicated the impossibility to process the request. The action to carry out by the UAC depends on the specific error report, e.g. reattempt the request later.</p>
500-599	<p>User Agent Server Error. This class of response indicates a system error which might occur, for instance, in a proxy server. The error could happen due to a congestion condition, overload, infrastructure problem, etc. Usually this error indicates that a particular proxy must be quarantined, i.e. the UA receiver of this response should not send a request to that proxy for a determined amount of time.</p>
600-699	<p>Global Error. This code range is SIP specific. It generally provides a relative response to the destination user, including a context of possible terminals for the related user. For example, the response could indicate that the user is unavailable in all its terminals.</p>

Table E - 3. SIP Status Code ranges and their meanings.

Just after the «Start Line», all SIP messages (either requests or responses) include a group of headers, some of them mandatory for each method (as seen in the corresponding table), while other are optional, the latter appearing only if necessary. A header field is composed by a field name, a colon and the header field value (which could also contain parameters preceded by a semicolon with the format «name=value»).

#### E.4.1.1.5.1 SIP Messages Header Fields

The header fields are used for means such as message routing, transaction identification, branch identification, path construction, dialog identification, subscriber contact and identification information exchange, etc.

Following are briefly described the mandatory header fields (for further detail refer to [29]):

- **To.** Specifies the logical recipient of the request.  
Example:  
**To:** Alice sip:Alice.Smith@domain.com
- **From.** Contains the URI of the user agent originating the request. In the same way as for the header field «To», its main use is for human consumption and filter purposes.  
Example:  
**From:** Bob <sip:Bob.Brown@domain2.com>;tag=9hx34576sl
- **Cseq.** Contains a sequence number in decimal numerical format and the application's method name (case-sensitive). They are used to match responses with requests within a SIP transaction, i.e. order transactions within a dialog, provide a means to uniquely identify transactions and differentiate between new requests and retransmissions.  
Example:  
**Cseq:** 21 INVITE
- **Call-ID:** It provides a unique identifier for an exchange of SIP messages. Uniquely identifies a particular invitation or all registrations of a user agent client in particular. A unique multimedia conference can carry multiple identifiers «Call-ID» (for example, if a user is invited on multiple occasions during the course of it). It may be represented just as «i».  
Example:  
**Call-ID:** f81d4fae-7dec-11d0-a765-00a0c91e6bf6@biloxi.com  
**i:** f81d4fae-7dec-11d0-a765-00a0c91e6bf6@192.0.2.4
- **Max-Forwards.** It is used to avoid routing loops. Each proxy handler demand this value decreases by one unit. If it reaches zero, the request is discarded.  
Ejemplo:  
**Max-Forwards:** 69
- **Via.** It keeps track of all proxies that the application has gone through. The response message uses this header field so as to pass through the same



proxy that the application has done before, but understandably in the opposite direction.

**Via:** SIP/2.0/UDP p1.domain.com:5060;branch=z9hG4bK543fg

**Via:** SIP/2.0/UDP ws.domain.com:5060;branch=z9hG4bK74gh5;received=10.0.0.2

#### **E.4.1.1.5.2 SIP Message Body**

The body of a SIP message (optional), preceded by a space line, follows the header fields. It is not used for routing a message or for transactional management. It normally contains application layer information, i.e. comprises the message payload to transfer between user agents between the ends of a SIP communication. A classic example of SIP body is constituted by «SDP» (Session Description Protocol).

SIP uses MIME (Multipurpose Internet Mail Extensions) for coding its messages. Consequently, the body of a SIP message is treated in the same way as an attachment within an email. Additionally, a group of header fields provide crucial information about the message body, namely:

- ✓ Content-Disposition
- ✓ Content-Type
- ✓ Content-Length

SIP methods will be described in examples throughout the rest of this section of the present document.

#### **E.4.1.1.5.3 SIP Methods Examples**

##### **E.4.1.1.5.3.1 SIP REGISTER**

The following example shows a SIP REGISTER of the user with address fernando@test.org and binds this address with the current location of it, i.e. the IP address 192.168.92.1, port 16036.

After the aforementioned successful registration, every attempt to connect the user of URI `sip:Fernando@test.org` will be redirected to the URI `sip:Fernando@192.168.93.1:16036`.

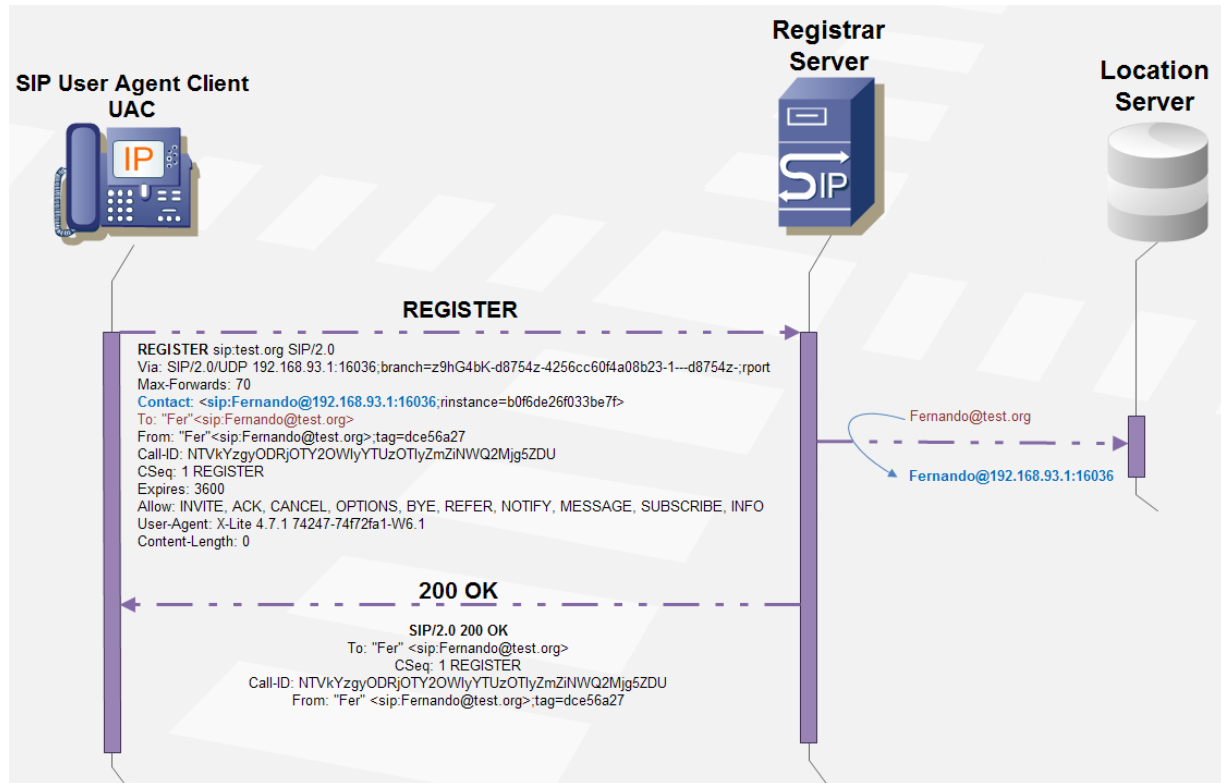


Figure E - 18. SIP REGISTER example.

#### E.4.1.1.5.3.2 SIP INVITE

The following figure depicts a conventional call with proxies according to [29]. INVITE, ACK and BYE methods are depicted.

The example only shows the two proxy servers involved in the overall transaction (as explained earlier, more could be involved in the session establishment).

As displayed, media is transmitted via RTP channels after the ACK transaction is completed.

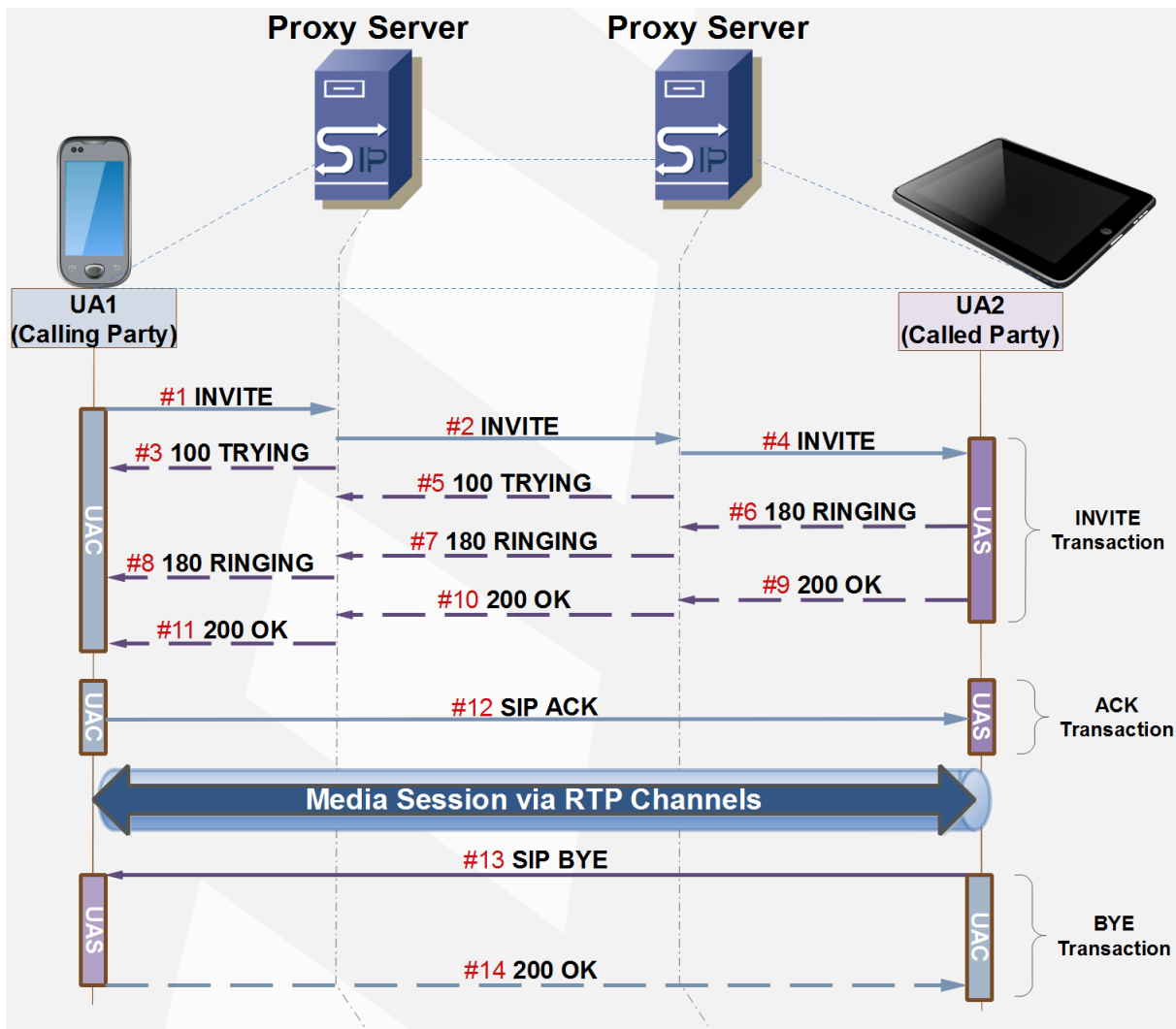


Figure E - 19. Conventional SIP call establishment with proxies.

Next two figures two modes of establishing a SIP call between SIP UAs: the proxy and the redirect mode.

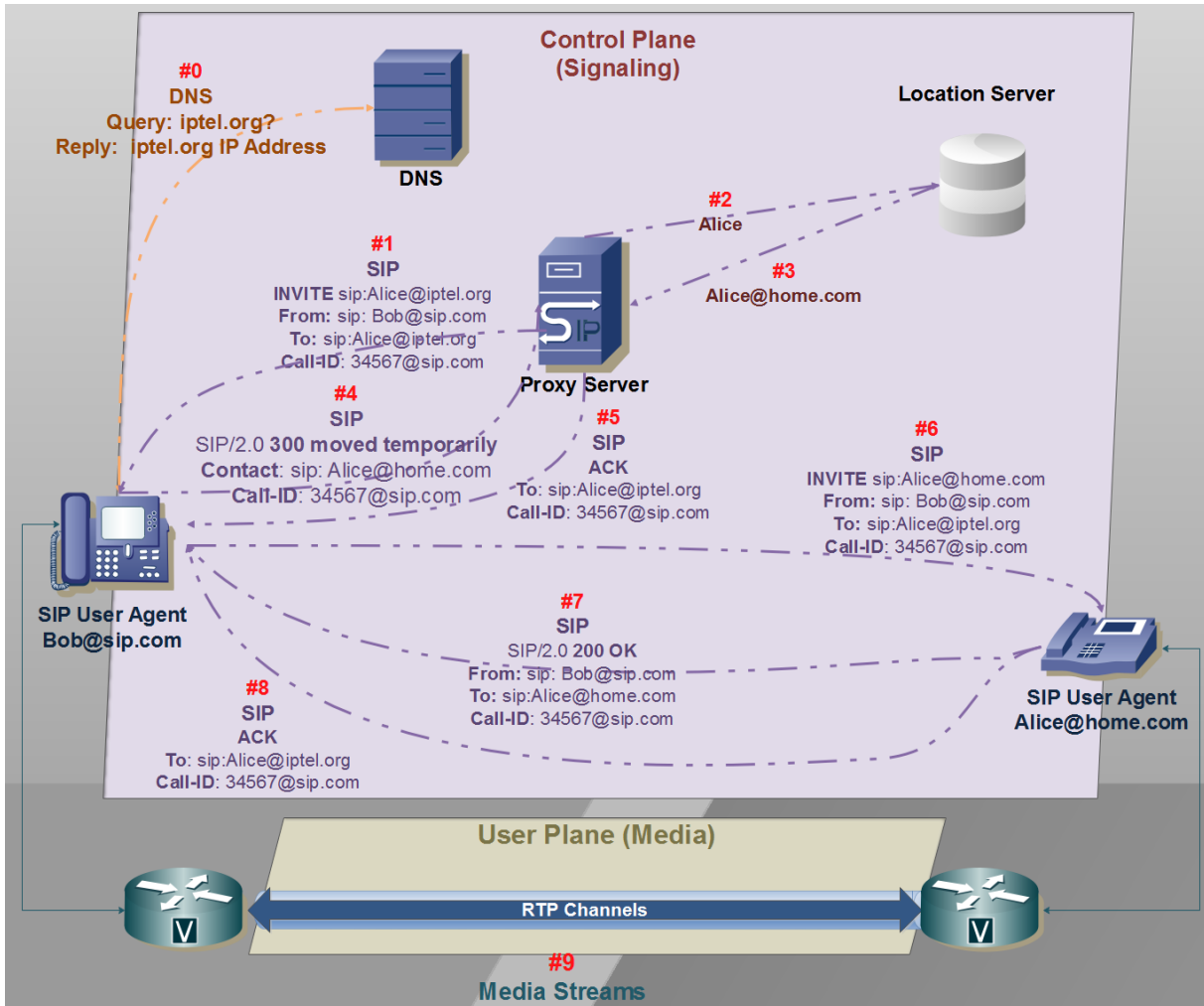


Figure E - 20. SIP call establishment: the proxy mode.

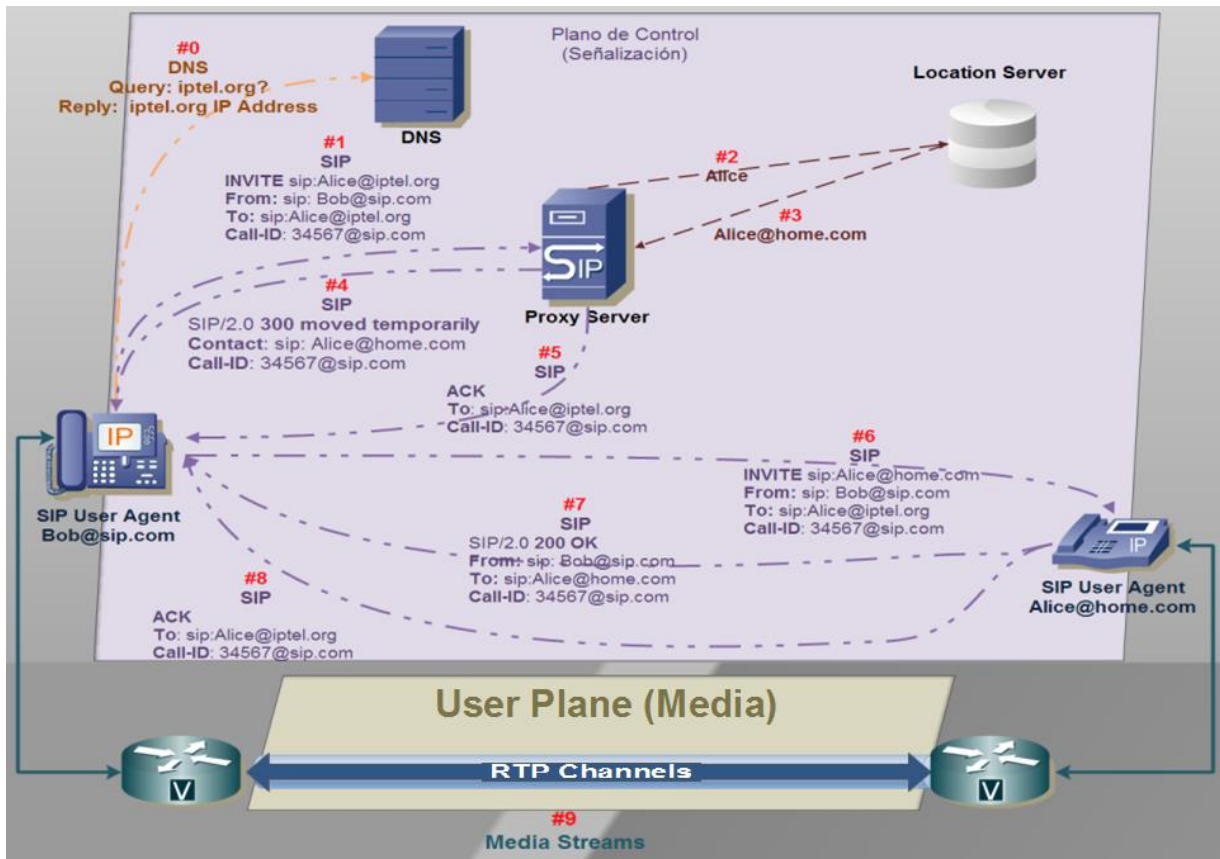


Figure E - 21. SIP call establishment: the redirect mode.

### E.4.1.1.5.3.3 SIP CANCEL

Next two figures show examples of the CANCEL method. While the first figure displays a normal CANCEL procedure, the second figure shows an example where messages cross deriving in the termination of the transaction through a BYE as explained earlier for this method when a final response was previously received. In the second figure the Cseq header field value takes an important role, so it is displayed along the whole message exchange.

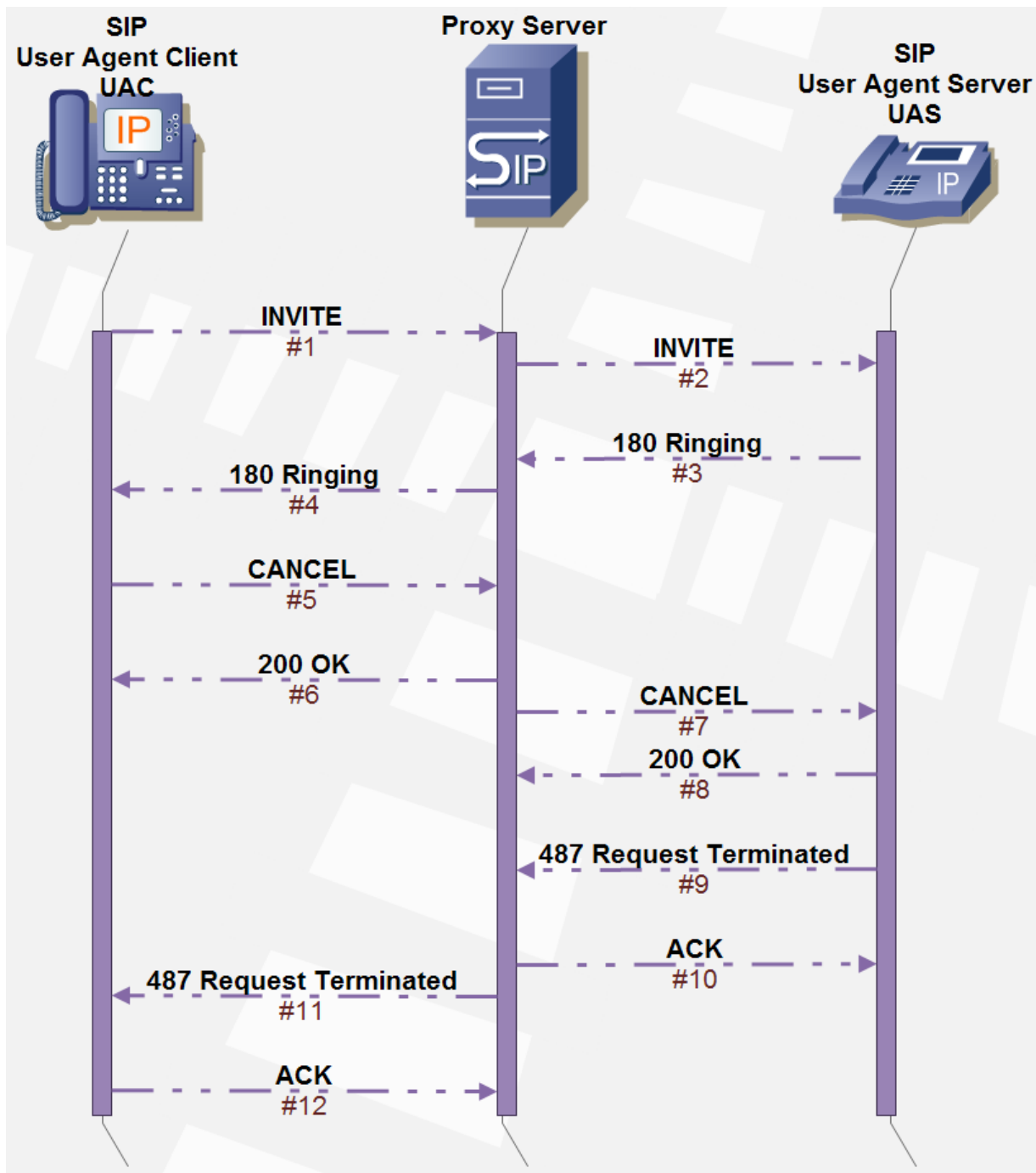


Figure E - 22. SIP CANCEL method normal procedure example.

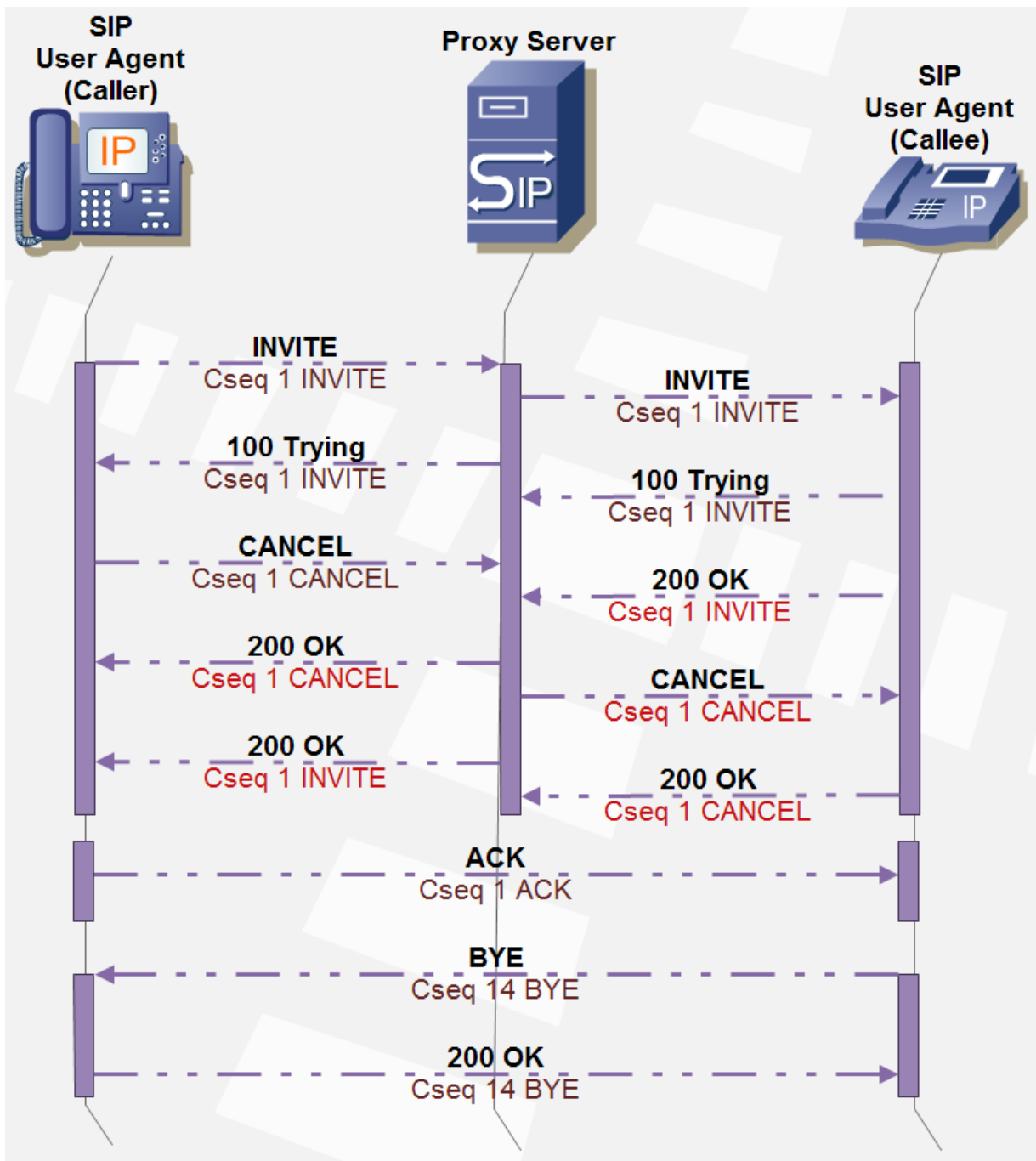


Figure E - 23. CANCEL method. Message cross example when a final response was previously received, deriving in termination via BYE.

#### E.4.1.1.5.3.4 SIP PRACK

Next figure shows a simple example of the PRACK method when nothing unusual happens during the SIP INVITE transaction.

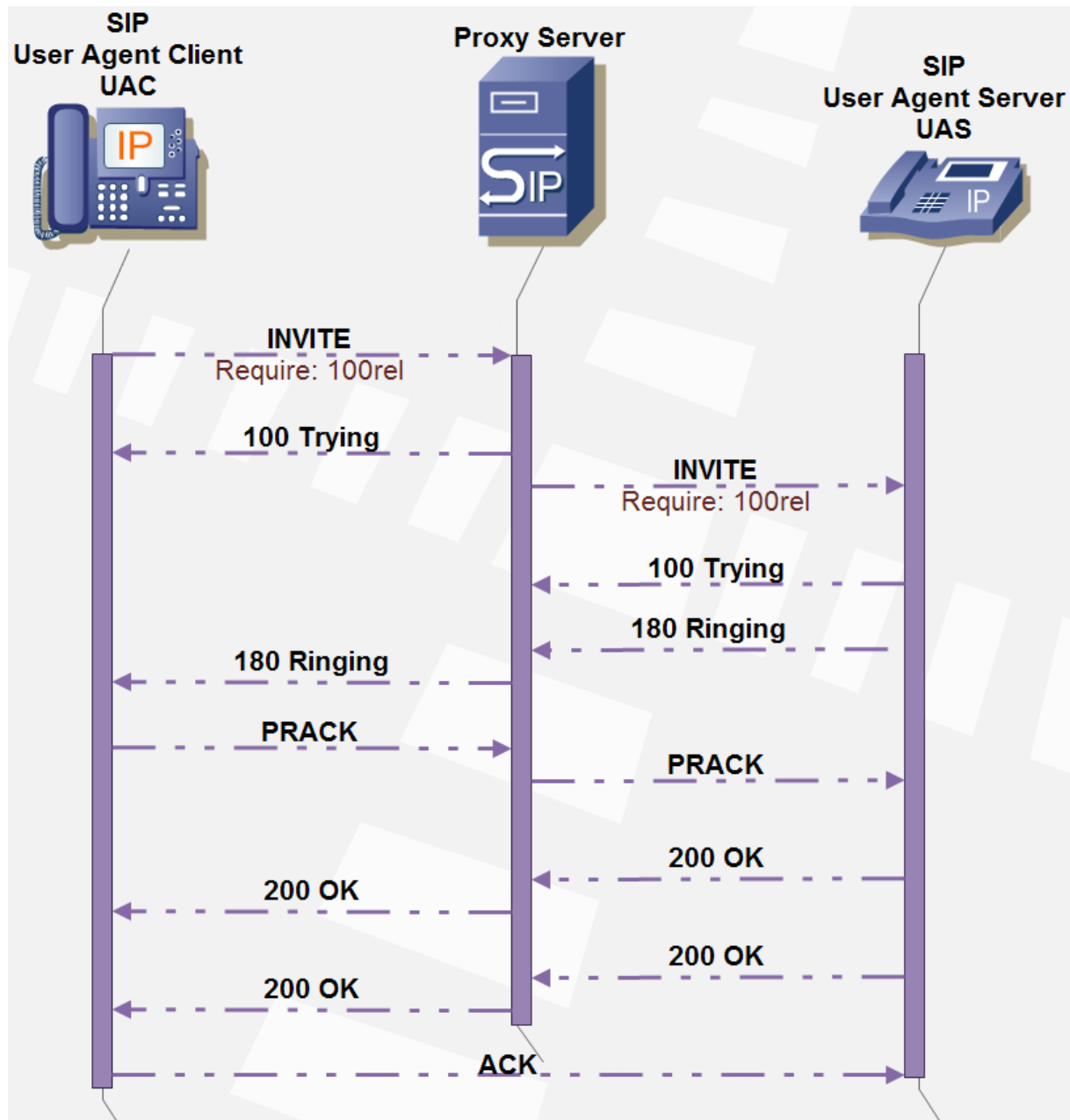


Figure E - 24. Simple PRACK method example during a SIP INVITE transaction.

In contrast, next figure shows a PRACK method example during a SIP INVITE transaction where a packet is lost. The Call-ID, CSeq and RACK header fields



combination allows the UAC correlate the PRACK with the provisional response it is acknowledging. Hence, all these parameter values are shown for better comprehension.

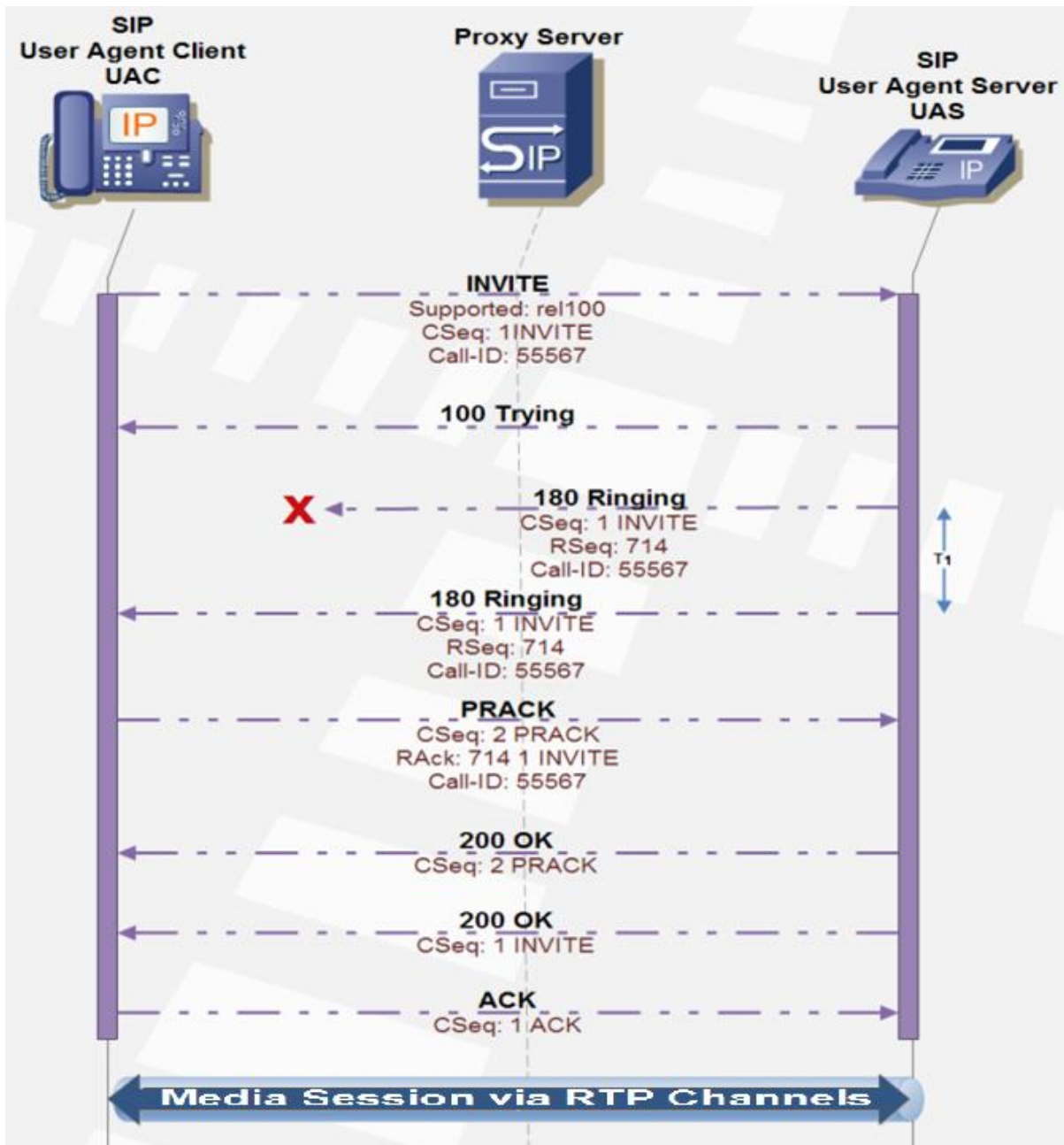


Figure E - 25. PRACK method example during a SIP INVITE transaction with a packet loss.

### E.4.1.1.5.3.5 SIP SUBSCRIBE / NOTIFY

Next figure displays normal SIP SUBSCRIBE / NOTIFY transactions.

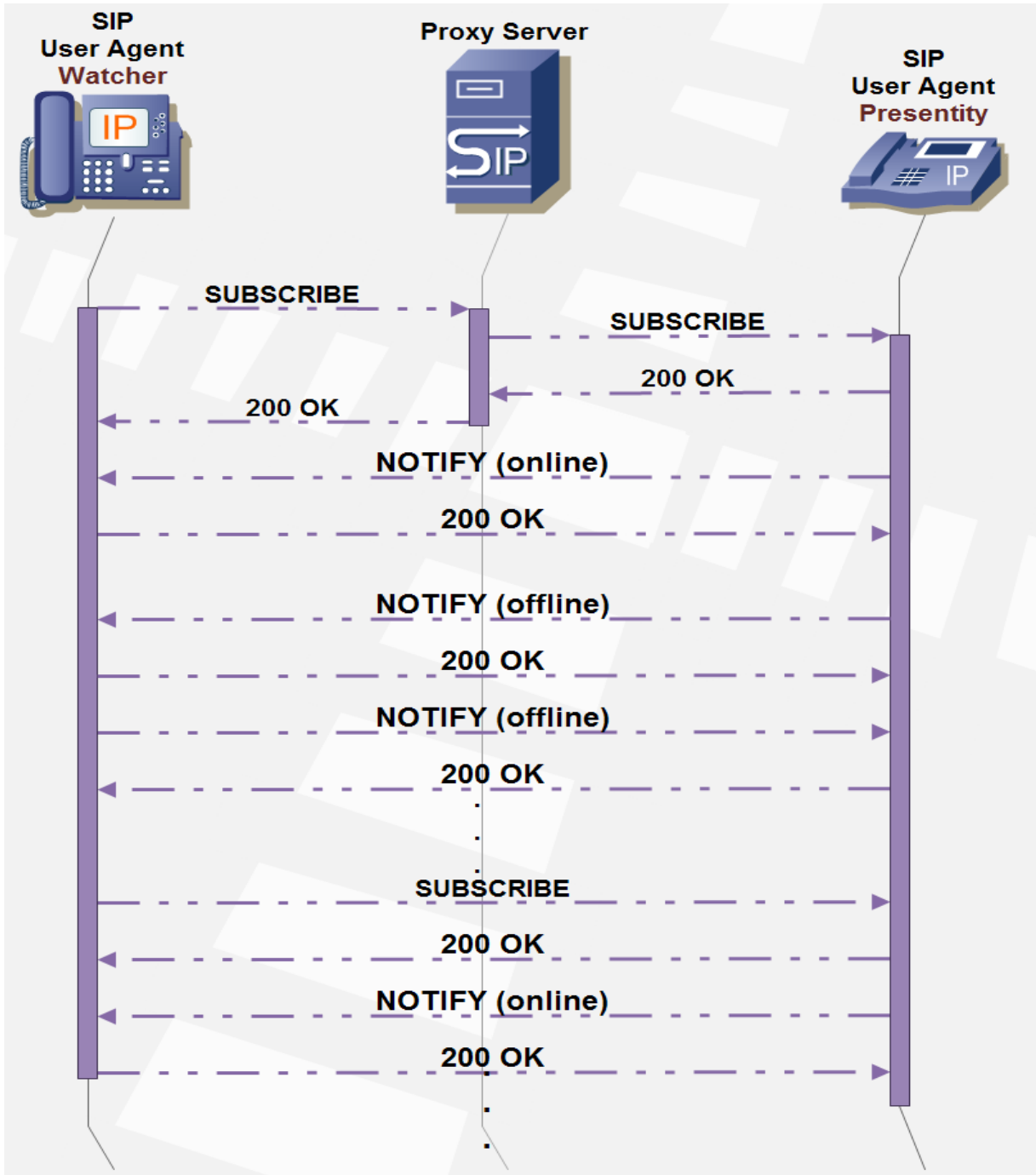


Figure E - 26. SIP SUBSCRIBE / NOTIFY normal transaction example.

### E.4.1.1.5.3.6 SIP PUBLISH

Next figure shows SIP PUBLISH method transaction and subsequent SIP NOTIFY transactions.

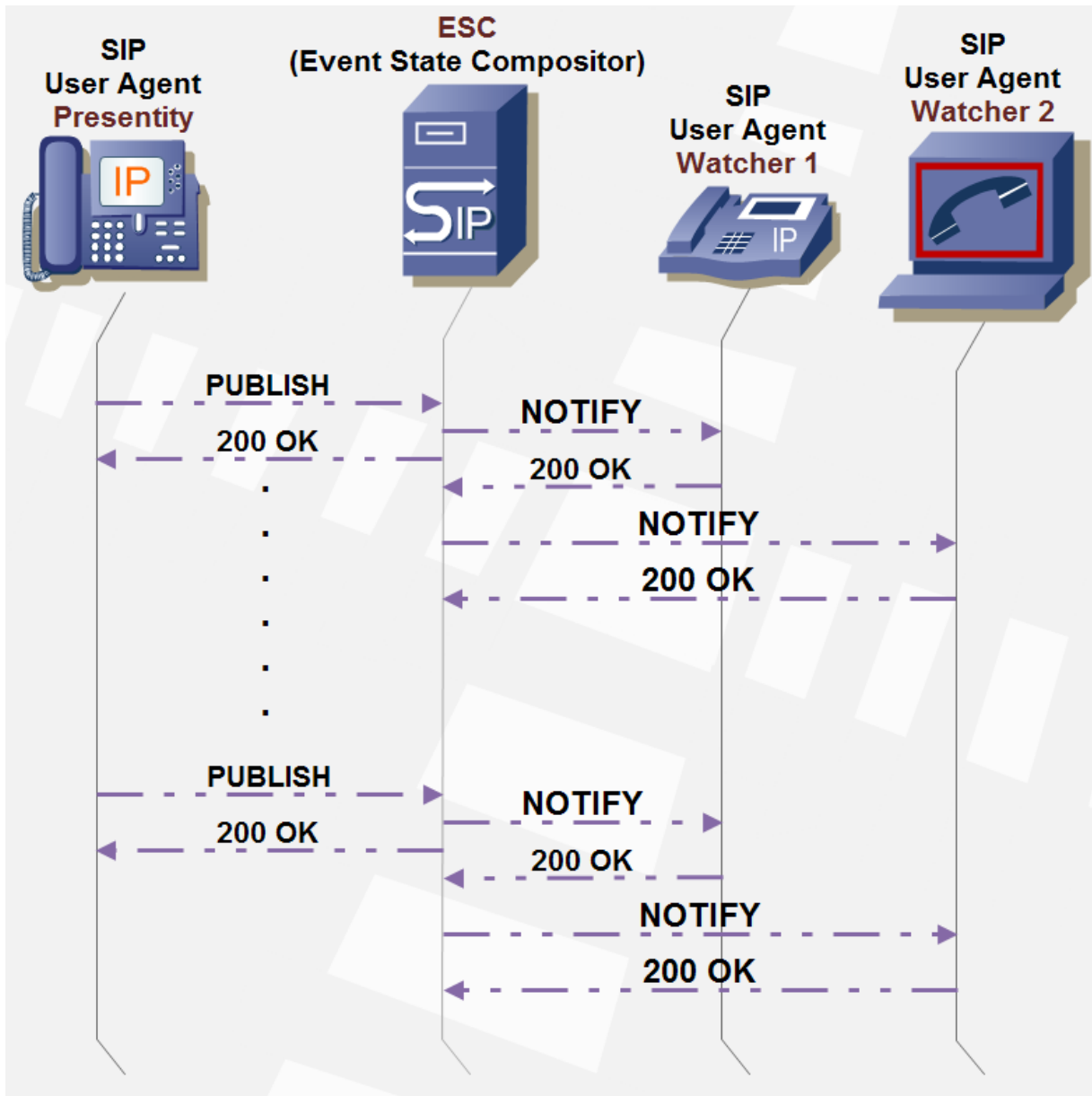


Figure E - 27. SIP PUBLISH / NOTIFY methods example.

### E.4.1.1.5.3.7 SIP UPDATE

Next figure displays an example of SIP UPDATE method for updating the QoS during a SIP INVITE transaction. Significant header field and SDP values are displayed for better comprehension of the example.

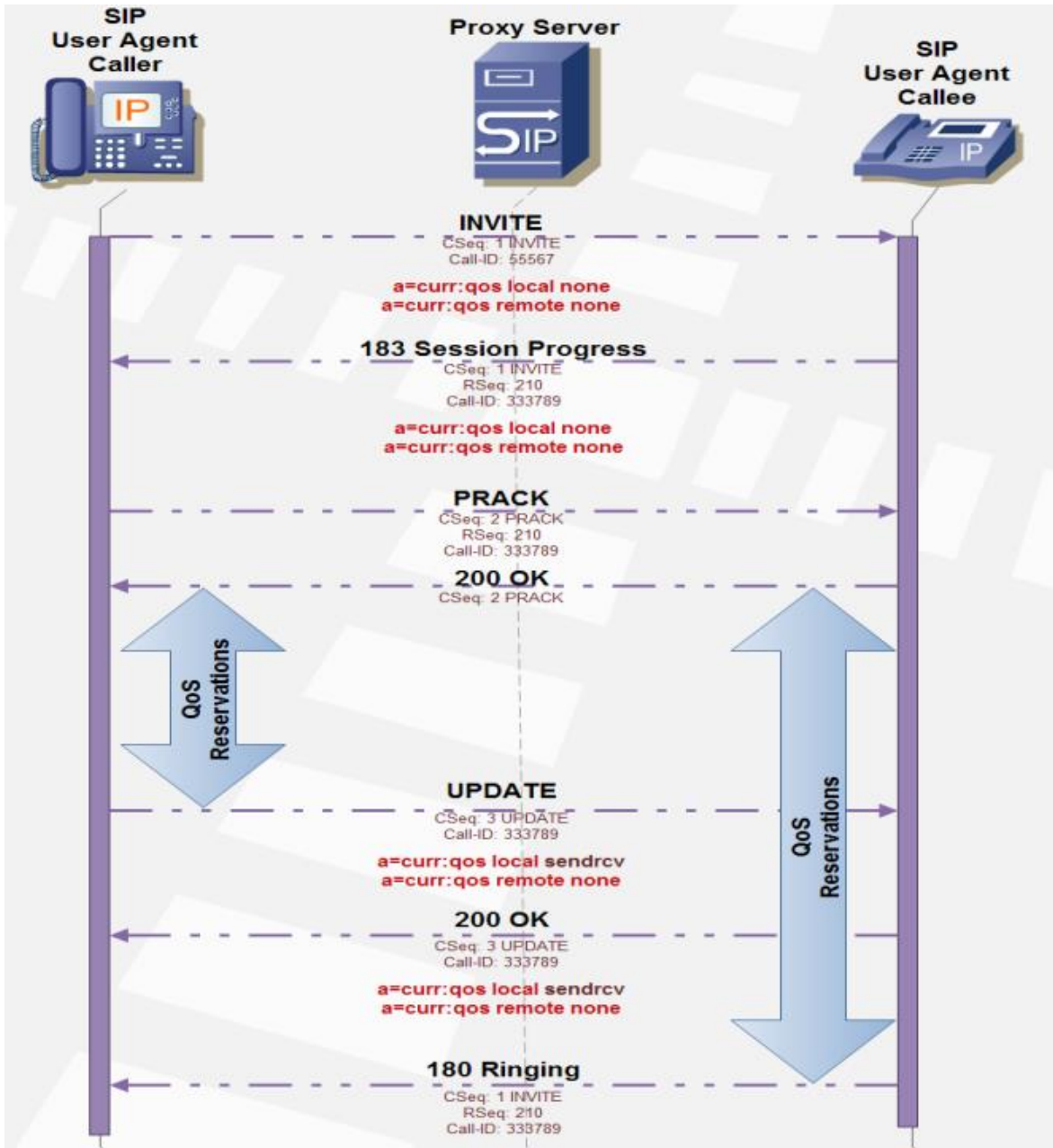


Figure E - 28. SIP UPDATE method example for QoS update during SIP INVITE transaction.

### E.4.1.1.5.3.8 SIP MESSAGE

Next figure shows SIP MESSAGE method transactions.

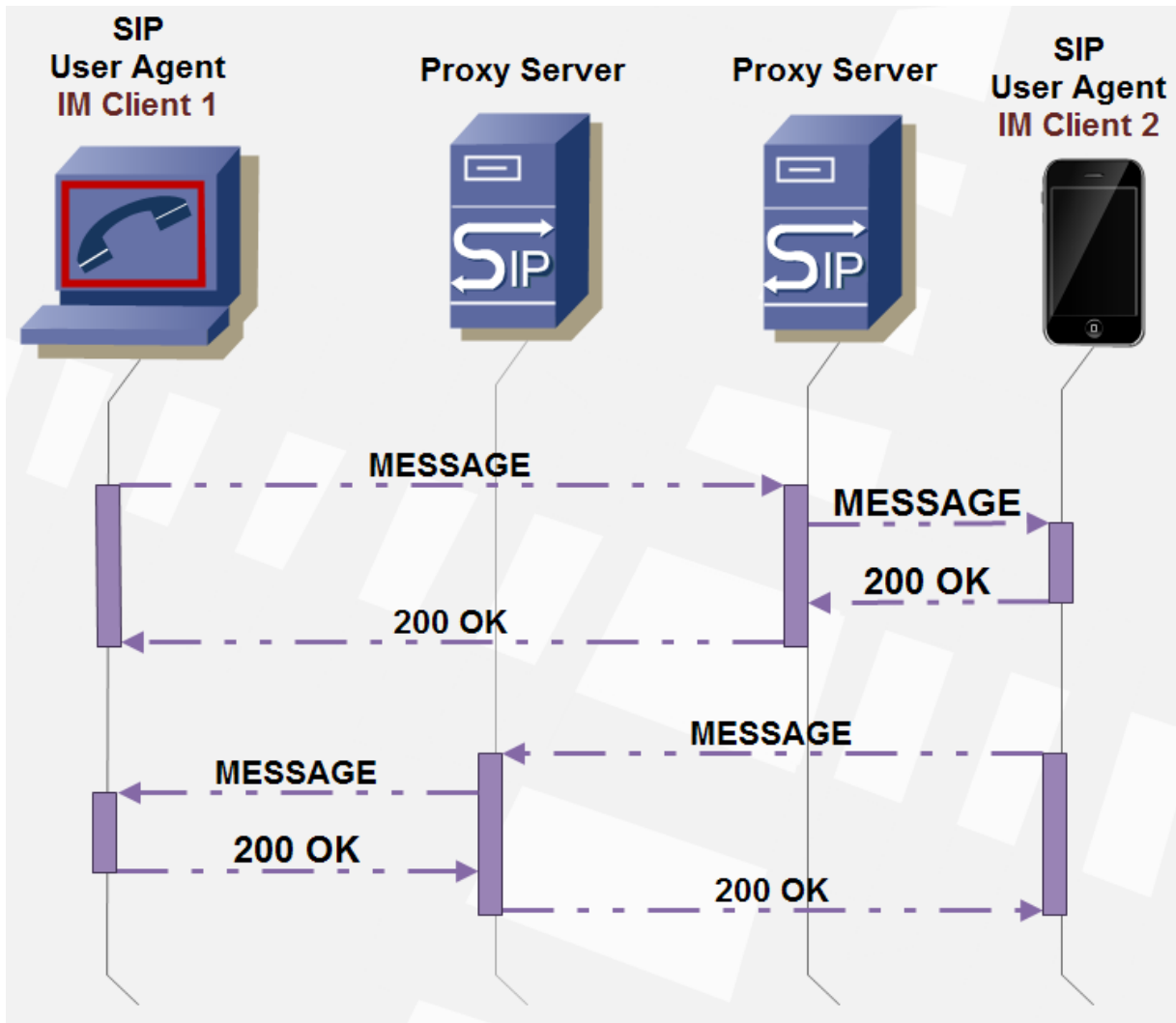


Figure E - 29. SIP MESSAGE method example.

### E.4.1.1.5.3.9 SIP REFER

Next three figures show use cases for the SIP REFER method. First example shows a call transfer. The second figure shows the use of the SIP REFER method for

retrieving a Web page via HTTP GET. Finally, the third figure shows the SIP REFER method use for call transfer with release from the user target of the transfer.

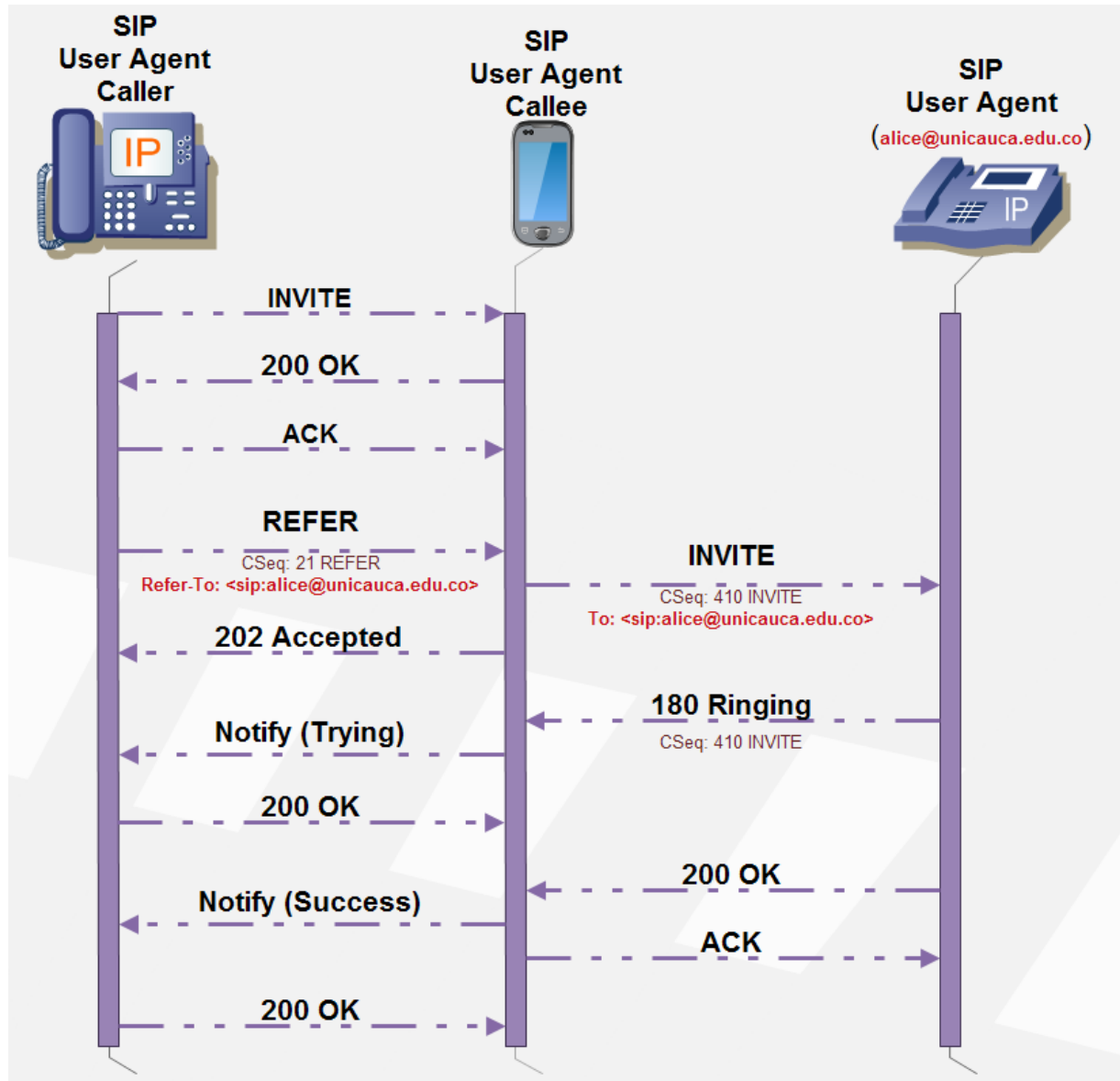


Figure E - 30. SIP REFER method example for call transference.

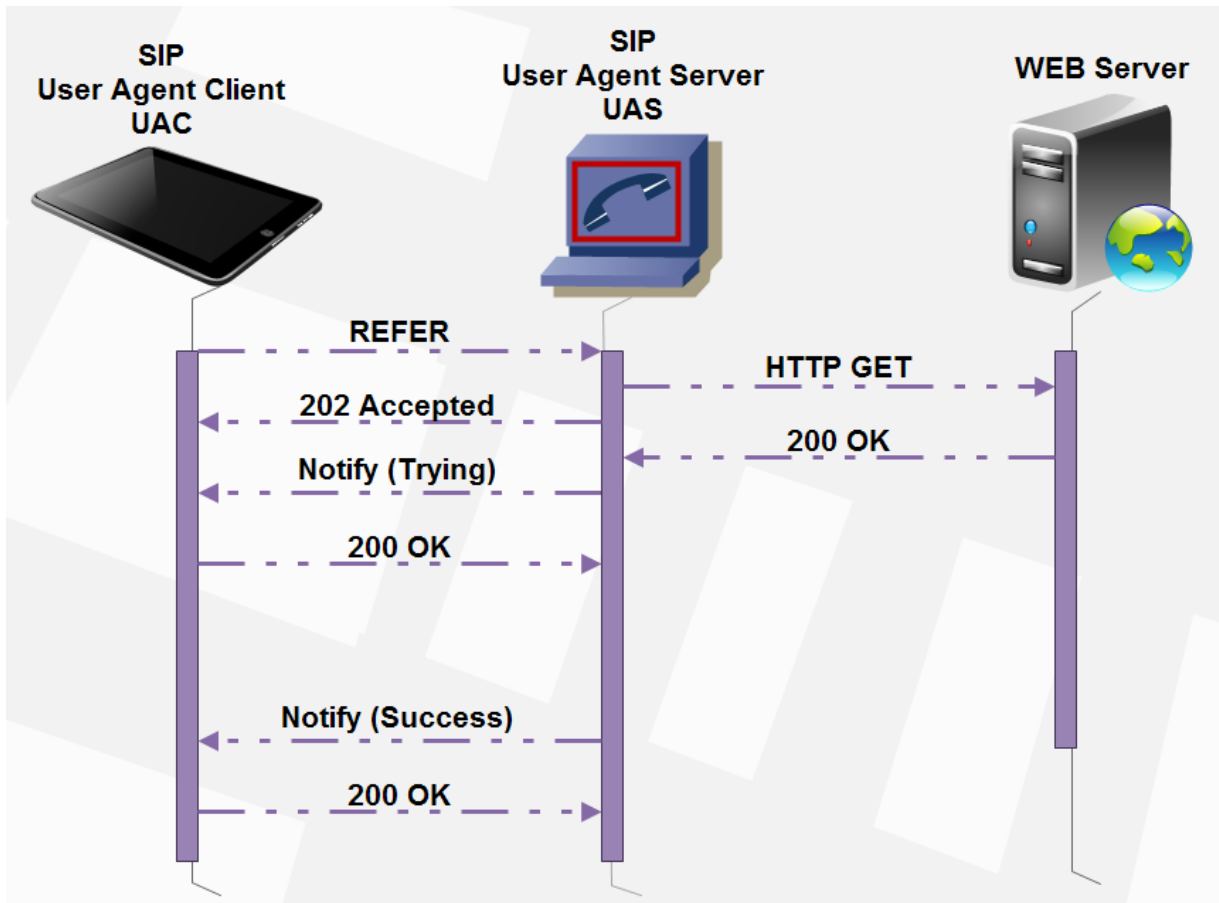


Figure E - 31. SIP REFER method example for Web Page retrieval through HTTP GET.

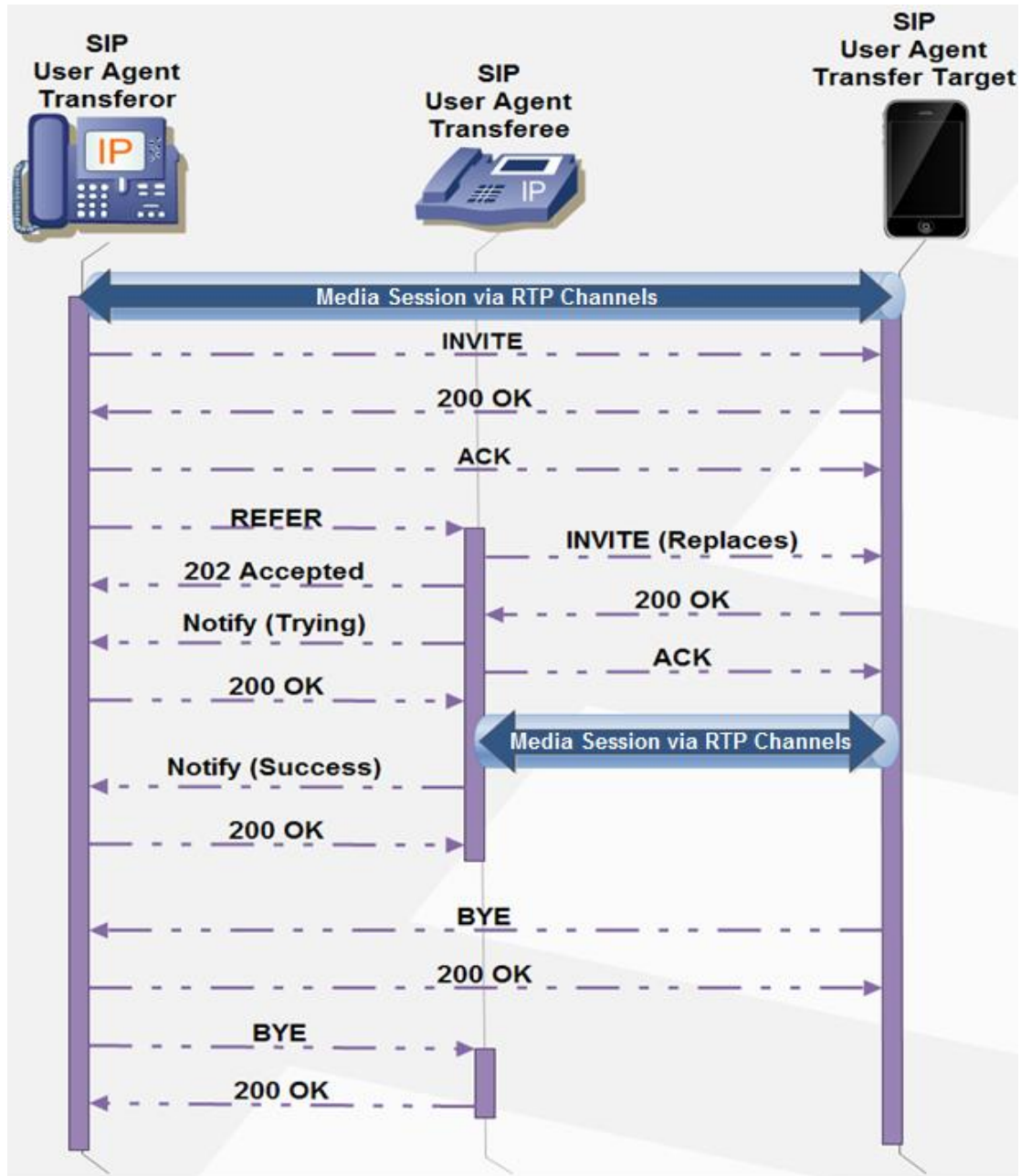


Figure E - 32. SIP REFER method example for call transfer with release from the user target of the transfer.



### E.4.1.1.6 USSD over SIP (USSI)

As specified in 3GPP TS 24.390 [42] and consistently with what's been described in sections 2.4 and 3.1 of this document, USSD for the IMS (and LTE) is embedded in a SIP message.

TeleStax Enterprise USSD Gateway translates USSD messages embedded in SS7 MAP operations to SIP or vice versa, according to 3GPP specs for either sides. As USSD payload is carried in XML within an HTTP message for the HTTP interface, in SIP messages it is carried as part of the body of the message as Content-Type «application/vnd.3gpp.ussd+xml».

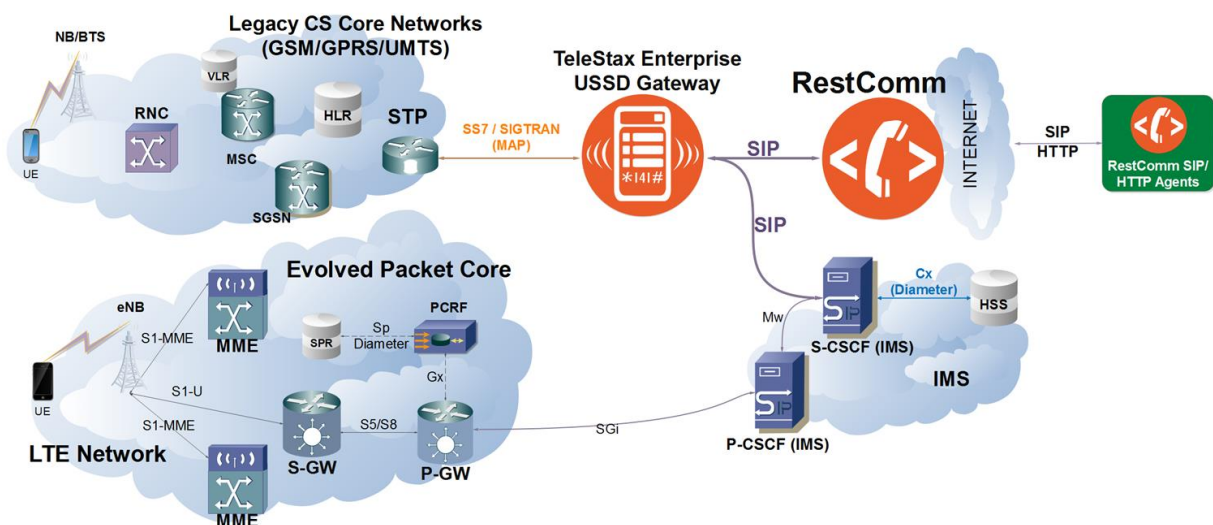


Figure E - 33. TeleStax Enterprise USSD Gateway between legacy SS7 and Next Generation Networks conveying USSD messages either over MAP or SIP correspondingly.

As described in Figure 3.4, which shows a USSD message sequence example between a User Equipment starting a service involving TeleStax Enterprise USSD Gateway, RestComm SIP Servlets and a third-party application. Following, traces of such example is shown, for a classic balance inquire service running USSD Gateway along with jSS7 simulator in the same machine, and RestComm in an Amazon EC2 instance, along with Apache Tomcat, PHP and MySQL for simulating an Online

Charging System. Traces are taken from Wireshark, worldwide most used open software protocol analyser (applying filter «sip || tcap »). Only SS7 MAP and SIP messages are included, thus showing the translation between each other and as for this annex purpose, how USSD is conveyed within SIP messages, or USSI as specified in [42]. As this annex treats about SIP, only SIP portions of following traces are highlighted in bold, as well as USSD payload within SIP messages.

No.	Time	Source	Destination	Protocol	Length	Info
176	96.854504729	1	2	GSM MAP	220	invoke processUnstructuredSS-Request

```

Frame 176: 220 bytes on wire (1760 bits), 220 bytes captured (1760 bits) on
interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Stream Control Transmission Protocol, Src Port: 8011 (8011), Dst Port: 8012 (8012)
MTP 3 User Adaptation Layer
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: invoke (1)
    invoke
      invokeID: 1
      opCode: localValue (0)
        localValue: processUnstructuredSS-Request (59)
      ussd-DataCodingScheme: 0f
        0000 .... = Coding Group: Coding Group 0(Language using the GSM 7
bit default alphabet) (0)
        .... 1111 = Language: Language unspecified (15)
      ussd-String: 2a994c3602
        USSD String: *222#

```

No.	Time	Source	Destination	Protocol	Length	Info
178	97.307504059	192.168.1.45	54.89.158.237	<b>SIP</b>	705	<b>Request: INVITE</b> sip:*222%23@54.89.158.237:5060

```

Frame 178: 705 bytes on wire (5640 bits), 705 bytes captured (5640 bits) on
interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.45, Dst: 54.89.158.237
User Datagram Protocol, Src Port: 5260, Dst Port: 5060
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:*222%23@54.89.158.237:5060 SIP/2.0
  Message Header
    Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45
    CSeq: 1 INVITE
    From: <sip:77390218@192.168.1.45:5260>;tag=2384
    To: <sip:*222%23@54.89.158.237:5060>
    Via: SIP/2.0/UDP 192.168.1.45:5260;rport;branch=z9hG4bK-333638-
6acc92d048bf6b9f7d1dbcce621e49d6

```

```

Max-Forwards: 70
Contact: "TelScaleUSSDGateway" <sip:77390218@192.168.1.45:5260>
Content-Type: application/vnd.3gpp.ussd+xml
Content-Length: 207
Message Body
<?xml version="1.0" encoding="UTF-8" ?>\n
<ussd-data>\n
\t<language value="en"/>\n
\t<ussd-string value="*222#"/>\n
\t<anyExt>\n
\t\t<message-type>processUnstructuredSSRequest_Request</message-type>\n
\t</anyExt>\n
</ussd-data>

```

No.	Time	Source	Destination	Protocol	Length	Info
179	97.614328303	54.89.158.237	192.168.1.45	SIP	484	Status: 180 Ringing

Frame 179: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 54.89.158.237, Dst: 192.168.1.45

User Datagram Protocol, Src Port: 5060, Dst Port: 5260

**Session Initiation Protocol (180)**

Status-Line: SIP/2.0 180 Ringing

Message Header

To:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a  
Via: SIP/2.0/UDP 192.168.1.45:5260;rport=5260;branch=z9hG4bK-333638-  
6acc92d048bf6b9f7d1dbcce621e49d6;received=167.56.163.173

CSeq: 1 INVITE

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

From: <sip:77390218@192.168.1.45:5260>;tag=2384

Server: TelScale Restcomm 7.9.0.1337

Contact: <sip:54.89.158.237:5060>

Content-Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
180	97.620811537	54.89.158.237	192.168.1.45	SIP	479	Status: 200 OK

Frame 180: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 54.89.158.237, Dst: 192.168.1.45

User Datagram Protocol, Src Port: 5060, Dst Port: 5260

**Session Initiation Protocol (200)**

Status-Line: SIP/2.0 200 OK

Message Header

To:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a  
Via: SIP/2.0/UDP 192.168.1.45:5260;rport=5260;branch=z9hG4bK-333638-  
6acc92d048bf6b9f7d1dbcce621e49d6;received=167.56.163.173

CSeq: 1 INVITE

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

```

From: <sip:77390218@192.168.1.45:5260>;tag=2384
Server: TelScale Restcomm 7.9.0.1337
Contact: <sip:54.89.158.237:5060>
Content-Length: 0

```

No.	Time	Source	Destination	Protocol	Length	Info
181	97.706168115	192.168.1.45	54.89.158.237	SIP	412	Request: ACK sip:54.89.158.237:5060

Frame 181: 412 bytes on wire (3296 bits), 412 bytes captured (3296 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.1.45, Dst: 54.89.158.237

User Datagram Protocol, Src Port: 5260, Dst Port: 5060

Session Initiation Protocol (ACK)

Request-Line: ACK sip:54.89.158.237:5060 SIP/2.0

Message Header

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

CSeq: 1 ACK

Via: SIP/2.0/UDP 192.168.1.45:5260;rport;branch=z9hG4bK-333638-ec5cb23242bddcbce0ef02bc2cce7132

From: <sip:77390218@192.168.1.45:5260>;tag=2384

To:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

Max-Forwards: 70

Content-Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
182	98.163748210	54.89.158.237	192.168.1.45	SIP	795	Request: INFO sip:77390218@167.56.163.173:5260

Frame 182: 795 bytes on wire (6360 bits), 795 bytes captured (6360 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 54.89.158.237, Dst: 192.168.1.45

User Datagram Protocol, Src Port: 5060, Dst Port: 5260

Session Initiation Protocol (INFO)

Request-Line: INFO sip:77390218@167.56.163.173:5260 SIP/2.0

Message Header

CSeq: 1 INFO

From:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

To: <sip:77390218@192.168.1.45:5260>;tag=2384

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

Max-Forwards: 70

User-Agent: TelScale Restcomm 7.9.0.1337

Via: SIP/2.0/UDP

54.89.158.237:5060;branch=z9hG4bKfc24853a\_57a5b08a\_e1de734b-3f6d-4207-b269-c339974195aa

Content-Type: application/vnd.3gpp.uspd+xml

Content-Length: 273

Message Body

<?xml version='1.0' encoding='UTF-8'?>\n

```

<ussd-data>\n
<language value="en"/>\n
<ussd-string value="Bienvenido 77390218 a su consulta de saldo Movistar.
Ingrese un digito para continuar"/>\n
<anyExt>\n
<message-type>unstructuredSSRequest_Request</message-type>\n
</anyExt>\n
</ussd-data>

```

No.	Time	Source	Destination	Protocol	Length	Info
183	98.273012491	192.168.1.45	54.89.158.237	SIP	384	Status: 200 OK

Frame 183: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.1.45, Dst: 54.89.158.237

User Datagram Protocol, Src Port: 5260, Dst Port: 5060

Session Initiation Protocol (200)

Status-Line: SIP/2.0 200 OK

Message Header

To: <sip:77390218@192.168.1.45:5260>;tag=2384

Via: SIP/2.0/UDP

54.89.158.237:5060;branch=z9hG4bKfc24853a\_57a5b08a\_e1de734b-3f6d-4207-b269-c339974195aa

CSeq: 1 INFO

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

From:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

Content-Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
184	98.334673331	2	1	GSM MAP	280	invoke unstructuredSS-Request

Frame 184: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Stream Control Transmission Protocol, Src Port: 8012 (8012), Dst Port: 8011 (8011)

MTP 3 User Adaptation Layer

Signalling Connection Control Part

Transaction Capabilities Application Part

GSM Mobile Application

Component: invoke (1)

invoke

invokeID: 1

opCode: localValue (0)

localValue: unstructuredSS-Request (60)

ussd-DataCodingScheme: 0f

0000 .... = Coding Group: Coding Group 0(Language using the GSM 7 bit default alphabet) (0)

.... 1111 = Language: Language unspecified (15)

ussd-String: c274d96d2fbbd3e437e8769be560b2180e1406cdeba0f1db...

USSD String: Bienvenido 77390218 a su consulta de saldo Movistar.  
 Ingrese un digito para continuar

No.	Time	Source	Destination	Protocol	Length	Info
200	117.562707980	1	2	GSM MAP	160	returnResultLast unstructuredSS-Request

Frame 200: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0  
 Linux cooked capture  
 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
 Stream Control Transmission Protocol, Src Port: 8011 (8011), Dst Port: 8012 (8012)  
 MTP 3 User Adaptation Layer  
 Signalling Connection Control Part  
 Transaction Capabilities Application Part  
 GSM Mobile Application  
 Component: returnResultLast (2)  
 returnResultLast  
 invokeID: 1  
 resultretres  
 opCode: localValue (0)  
 localValue: unstructuredSS-Request (60)  
 ussd-DataCodingScheme: 0f  
 0000 .... = Coding Group: Coding Group 0(Language using the GSM 7 bit default alphabet) (0)  
 .... 1111 = Language: Language unspecified (15)  
 ussd-String: 33  
 USSD String: 3

No.	Time	Source	Destination	Protocol	Length	Info
201	117.625017441	192.168.1.45	54.89.158.237	SIP	658	Request: INFO sip:54.89.158.237:5060

Frame 201: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits) on interface 0  
 Linux cooked capture  
 Internet Protocol Version 4, Src: 192.168.1.45, Dst: 54.89.158.237  
 User Datagram Protocol, Src Port: 5260, Dst Port: 5060  
**Session Initiation Protocol (INFO)**  
 Request-Line: INFO sip:54.89.158.237:5060 SIP/2.0  
 Message Header  
 CSeq: 2 INFO  
 From: <sip:77390218@192.168.1.45:5260>;tag=2384  
 To:  
 <sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a  
 Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45  
 Max-Forwards: 70  
 Via: SIP/2.0/UDP 192.168.1.45:5260;rport;branch=z9hG4bK-333638-4fc9a99bc245ea16fa3f31b3d567da6d  
 Content-Type: application/vnd.3gpp.ussd+xml  
 Content-Length: 197  
 Message Body

```
<?xml version="1.0" encoding="UTF-8" ?>\n
<ussd-data>\n
\t<language value="en"/>\n
\t<ussd-string value="3"/>\n
\t<anyExt>\n
\t\t<message-type>unstructuredSSRequest_Response</message-type>\n
\t</anyExt>\n
</ussd-data>
```

No.	Time	Source	Destination	Protocol	Length	Info
203	117.823626434	54.89.158.237	192.168.1.45	SIP	477	Status: 200 OK

Frame 203: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 54.89.158.237, Dst: 192.168.1.45

User Datagram Protocol, Src Port: 5060, Dst Port: 5260

**Session Initiation Protocol (200)**

Status-Line: SIP/2.0 200 OK

Message Header

To:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a  
Via: SIP/2.0/UDP 192.168.1.45:5260;rport=5260;branch=z9hG4bK-333638-4fc9a99bc245ea16fa3f31b3d567da6d;received=167.56.163.173

CSeq: 2 INFO

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

From: <sip:77390218@192.168.1.45:5260>;tag=2384

Server: TelScale Restcomm 7.9.0.1337

Contact: <sip:54.89.158.237:5060>

Content-Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
204	117.984537866	54.89.158.237	192.168.1.45	SIP	814	Request: INFO sip:77390218@167.56.163.173:5260

Frame 204: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 54.89.158.237, Dst: 192.168.1.45

User Datagram Protocol, Src Port: 5060, Dst Port: 5260

**Session Initiation Protocol (INFO)**

Request-Line: INFO sip:77390218@167.56.163.173:5260 SIP/2.0

Message Header

CSeq: 2 INFO

From:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

To: <sip:77390218@192.168.1.45:5260>;tag=2384

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

Max-Forwards: 70

User-Agent: TelScale Restcomm 7.9.0.1337

Via: SIP/2.0/UDP

54.89.158.237:5060;branch=z9hG4bKfc24853a\_57a5b08a\_27beddad-bff9-4492-a506-befe33bbbf7d

```

Content-Type: application/vnd.3gpp.usss+xml
Content-Length: 292
Message Body
<?xml version='1.0' encoding='UTF-8'?>\n
<ussd-data>\n
<language value="en"/>\n
<ussd-string value="Su saldo de voz es: $ 20.91. Para consultar su saldo
de datos digite 1, para SMS digite 2, para salir 0."/>\n
<anyExt>\n
<message-type>unstructuredSSRequest_Request</message-type>\n
</anyExt>\n
</ussd-data>

```

No.	Time	Source	Destination	Protocol	Length	Info
205	117.995686184	192.168.1.45	54.89.158.237	SIP	384	Status: 200 OK

Frame 205: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.1.45, Dst: 54.89.158.237

User Datagram Protocol, Src Port: 5260, Dst Port: 5060

Session Initiation Protocol (200)

Status-Line: SIP/2.0 200 OK

Message Header

To: <sip:77390218@192.168.1.45:5260>;tag=2384

Via: SIP/2.0/UDP

54.89.158.237:5060;branch=z9hG4bKfc24853a\_57a5b08a\_27beddad-bff9-4492-a506-befe33bbbf7d

CSeq: 2 INFO

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

From:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

Content-Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
206	118.012877505	2	1	GSM MAP	252	invoke unstructuredSS-Request

Frame 206: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Stream Control Transmission Protocol, Src Port: 8012 (8012), Dst Port: 8011 (8011)

MTP 3 User Adaptation Layer

Signalling Connection Control Part

Transaction Capabilities Application Part

GSM Mobile Application

Component: invoke (1)

invoke

invokeID: 2

opCode: localValue (0)

localValue: unstructuredSS-Request (60)

ussd-DataCodingScheme: 0f



```

    0000 .... = Coding Group: Coding Group 0(Language using the GSM 7
bit default alphabet) (0)
    .... 1111 = Language: Language unspecified (15)
    ussd-String: d33a681e6693df207219647feb41e5b90e2400c960ae5ccc...
    USSD String: Su saldo de voz es: $ 20.91. Para consultar su saldo
de datos digite 1, para SMS digite 2, para salir 0.

```

No.	Time	Source	Destination	Protocol	Length	Info
318	133.803354888	1	2	GSM MAP	160	returnResultLast unstructuredSS-Request

```

Frame 318: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on
interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Stream Control Transmission Protocol, Src Port: 8011 (8011), Dst Port: 8012 (8012)
MTP 3 User Adaptation Layer
Signalling Connection Control Part
Transaction Capabilities Application Part
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
      invokeID: 2
      resultretres
        opCode: localValue (0)
          localValue: unstructuredSS-Request (60)
            ussd-DataCodingScheme: 0f
              0000 .... = Coding Group: Coding Group 0(Language using the
GSM 7 bit default alphabet) (0)
              .... 1111 = Language: Language unspecified (15)
              ussd-String: 30
              USSD String: 0

```

No.	Time	Source	Destination	Protocol	Length	Info
319	133.847669752	192.168.1.45	54.89.158.237	SIP	658	Request: INFO sip:54.89.158.237:5060

```

Frame 319: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits) on
interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.45, Dst: 54.89.158.237
User Datagram Protocol, Src Port: 5260, Dst Port: 5060
Session Initiation Protocol (INFO)
  Request-Line: INFO sip:54.89.158.237:5060 SIP/2.0
  Message Header
    CSeq: 3 INFO
    From: <sip:77390218@192.168.1.45:5260>;tag=2384
    To:
<sip:*222%23@54.89.158.237:5060>;tag=54994938_2b4303c7_57a5b08a_fc24853a
    Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45
    Max-Forwards: 70
    Via: SIP/2.0/UDP 192.168.1.45:5260;rport;branch=z9hG4bK-333638-
0925d2b4783744eb431430daafe2b509

```

```

Content-Type: application/vnd.3gpp.usss+xml
Content-Length: 197
Message Body
<?xml version="1.0" encoding="UTF-8" ?>\n
<ussd-data>\n
\t<language value="en"/>\n
\t<ussd-string value="0"/>\n
\t<anyExt>\n
\t\t<message-type>unstructuredSSRequest_Response</message-type>\n
\t</anyExt>\n
</ussd-data>

```

No.	Time	Source	Destination	Protocol	Length	Info
321	134.036930750	54.89.158.237	192.168.1.45	SIP	477	Status: 200 OK

Frame 321: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 54.89.158.237, Dst: 192.168.1.45

User Datagram Protocol, Src Port: 5060, Dst Port: 5260

**Session Initiation Protocol (200)**

Status-Line: SIP/2.0 200 OK

Message Header

To:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

Via: SIP/2.0/UDP 192.168.1.45:5260;rport=5260;branch=z9hG4bK-333638-0925d2b4783744eb431430daafe2b509;received=167.56.163.173

CSeq: 3 INFO

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

From: <sip:77390218@192.168.1.45:5260>;tag=2384

Server: TelScale Restcomm 7.9.0.1337

Contact: <sip:54.89.158.237:5060>

Content-Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
322	134.058990545	54.89.158.237	192.168.1.45	SIP	767	Request: BYE sip:77390218@167.56.163.173:5260

Frame 322: 767 bytes on wire (6136 bits), 767 bytes captured (6136 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 54.89.158.237, Dst: 192.168.1.45

User Datagram Protocol, Src Port: 5060, Dst Port: 5260

**Session Initiation Protocol (BYE)**

Request-Line: BYE sip:77390218@167.56.163.173:5260 SIP/2.0

Message Header

CSeq: 3 BYE

From:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

To: <sip:77390218@192.168.1.45:5260>;tag=2384

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

Max-Forwards: 70

User-Agent: TelScale Restcomm 7.9.0.1337

```

Via: SIP/2.0/UDP
54.89.158.237:5060;branch=z9hG4bKfc24853a_57a5b08a_5dc3be9b-b3a5-4d17-83be-
07f263246b96
Content-Type: application/vnd.3gpp.ussd+xml
Content-Length: 247
Message Body
<?xml version='1.0' encoding='UTF-8'?>\n
<ussd-data>\n
<language value="en"/>\n
<ussd-string value="Gracias por utilizar su consulta de saldo
Movistar!"/>\n
<anyExt>\n
<message-type>processUnstructuredSSRequest_Response</message-type>\n
</anyExt>\n
</ussd-data>

```

No.	Time	Source	Destination	Protocol	Length	Info
323	134.066647939	192.168.1.45	54.89.158.237	SIP	383	Status: 200 OK

Frame 323: 383 bytes on wire (3064 bits), 383 bytes captured (3064 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 192.168.1.45, Dst: 54.89.158.237

User Datagram Protocol, Src Port: 5260, Dst Port: 5060

**Session Initiation Protocol (200)**

Status-Line: SIP/2.0 200 OK

Message Header

To: <sip:77390218@192.168.1.45:5260>;tag=2384

Via: SIP/2.0/UDP

54.89.158.237:5060;branch=z9hG4bKfc24853a\_57a5b08a\_5dc3be9b-b3a5-4d17-83be-07f263246b96

CSeq: 3 BYE

Call-ID: a03efa566dc99947f37c943ccd6874b0@192.168.1.45

From:

<sip:\*222%23@54.89.158.237:5060>;tag=54994938\_2b4303c7\_57a5b08a\_fc24853a

Content-Length: 0

No.	Time	Source	Destination	Protocol	Length	Info
324	134.084025015	2	1	GSM MAP	200	returnResultLast processUnstructuredSS-Request

Frame 324: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Stream Control Transmission Protocol, Src Port: 8012 (8012), Dst Port: 8011 (8011)

MTP 3 User Adaptation Layer

Signalling Connection Control Part

Transaction Capabilities Application Part

GSM Mobile Application

Component: returnResultLast (2)

returnResultLast

invokeID: 1

```

resultretres
  opCode: localValue (0)
    localValue: processUnstructuredSS-Request (59)
  ussd-DataCodingScheme: 0f
    0000 .... = Coding Group: Coding Group 0(Language using the
GSM 7 bit default alphabet) (0)
    .... 1111 = Language: Language unspecified (15)
  ussd-String: 4779789c0ecf41f0b71c54a7a7d9697d580e9ad741e3b77b...
    USSD String: Gracias por utilizar su consulta de saldo
Movistar!

```

## E.4.2 VoIP User Plane Protocols

### E.4.2.1 Real-time Transport Protocol (RTP)

Specified by IETF RFC 3550, provides audio/video flow transmission in real time over IP networks with following main characteristics:

- ✓ Packet sequence.
- ✓ Intra-media synchronicity.
- ✓ Inter-media synchronicity.
- ✓ Payload identification.
- ✓ Frame indication.

RTP does not reserve resources or guarantees quality (QoS) of service in real time, given it prioritize speed rather than QoS. Then, it uses non-reliable transport protocols such as UDP or DCCP (Datagram Congestion Control Protocol -IETF RFC 4340-).

RTP is always is together with RTCP (RTP Control Protocol), which provides QoS statistics and synchronicity internal media information. Both are designed to work independently from the underlying networks and transport means.

Given the fact that IP network do not keep a relationship with the transported data (i.e. they introduce jitter), the main purpose of RTP is allowing the receivers to reproduce the media information at the appropriate pace. In other words, in the case

of two packets being sent to the same destination with a time span of exactly N milliseconds, nothing assures that the second packet will arrive before, simultaneously or after the first one. Then, receivers cannot trust in packet arrival times.

So as to recovering the time relationship of media packets, «RTP timestamps» are used. The receivers place the RTP packets in the buffer according to these timestamps and reproduce them consequently. If a packet with a particular timestamp needs to be reproduced and has not yet arrived, the receiver used interpolation techniques to fill the void (e.g. for audio, it could reproduce the last audio packet for a longer time). In case that this packet is received after the time it was meant to be reproduced, it is discarded. The RTP receiver need to make a decision: when start reproducing media to the user. It then faces a tradeoff solution, both with risks, namely:

- a) Start immediately when receiving the first packet, risking loosing QoS afterwards due to packet loss.
- b) If it holds before reproducing, the delay could be so big that the users could end up being unable to sustain a normal conversation (the buffer should be augmented in this case for compensation).

Two types of implementations exist which use different criteria for deciding buffer length:

- Big buffers enhance QoS but increase delays.
- Small buffers decrease delays but QoS is deteriorated.

Delay experimented by a packet burst between transmitter and receiver normally has a Gaussian distribution. Then, the majority of the packets arrive close to a certain moment in time. For example, imagine a scenario where this delay is about 50 ms. An Acceptable tradeoff solution for this example would be that the receiver starts reproducing the packets 100 ms after transmission. By this way, only a small fraction of the received packets would be discarded on arrival.

Additional to timestamps, RTP packets may be transported in sequence (but not for packet retransmission, as RTP uses non-reliable transport protocols like UDP, given the fact that it prioritizes speed rather than QoS, i.e. the reproduction of the

received information in real time over the security of data arrival, given the nature of the service for which it is designed for). The receivers use eventual sequence numbers so as to understand how many packets are lost in the network during the transmission. If the network loses too much packets in a given time, the peers could actually decide to use a codec with improved redundancy for providing a better QoS under high loss conditions.

Payload types are referred by numbers. For example, «payload type 0» corresponds to ITU-T G.711 Codec according to  $\mu$  law, meanwhile «payload type 31» corresponds to ITU-T H.264 Video Codec. IETF RFC 3551 defines some of the types of audio and video fixed payloads.

Dynamic types of payload typically are negotiated by the offer/response model. They identify a specific codec for a particular session. This is done typically during session initiation through SDP within SIP in the control plane, like in the next example:

```
v=0
o=Alice 2790844676 2867892807 IN IP4 192.0.0.1
s=Let's talk
c=IN IP4 192.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0 98
a=rtpmap:98 L16/16000/2
```

#### E.4.2.1.1 RTP Packet Structure



Figure E - 34. RTP packet example transporting an audio sample via UDP.

Figure E-31 displays an RTP packet structure example, which comprises the following header fields:

- **Version (V):** This 2-bit field identifies the RTP version. As for IETF RFC 3550 this value must always be set to «2».
- **Padding (P):** If set to «1», the packet contains one or more additional padding octets. Last padding octet keeps an account of how many padding octets shall be ignored, including itself. The padding may be needed for some encrypting algorithms for fixed size blocks, or for transporting multiple RTP packets in a lower layer data unit.
- **Extension (X):** If set to «1», the fixed header must be followed by exactly one header extension.
- **CSRC Count (CC):** This 4-bit field contains the CSRC identifiers that follow the fixed header.
- **Marker (M):** The interpretation of the marker bit is defined by a profile. It is intended to allow significant events such as frame boundaries to be marked in the packet stream. A profile may define additional marker bits or define that there is no marker bit by changing the number of bits in the payload type field (PT).
- **Payload Type (PT):** This 7-bit field identifies the format of the RTP payload and determines its interpretation by the application. A profile may specify a default static mapping of payload type codes to payload formats. Additional payload type codes may be defined dynamically through non-RTP means. A set of default mappings for audio and video is specified in the companion RFC 3551. An RTP source may change the payload type during a session, but this field should not be used for multiplexing separate media streams. A receiver must ignore packets with payload types that it does not understand.
- **Sequence Number:** This 16 bit-field field constitutes a sequence number which increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss and to restore packet sequence. The initial value of the sequence number should be random to make known-plain text attacks on encryption more difficult.

- **Timestamp:** This 32 bit-field reflects the sampling instant of the first octet in the RTP data packet. The sampling instant must be derived from a clock that increments monotonically and linearly in time to allow synchronization and jitter calculations. The resolution of the clock must be sufficient for the desired synchronization accuracy and for measuring packet arrival jitter. The clock frequency is dependent on the format of data carried as payload and is specified statically in the profile or payload format specification that defines the format, or may be specified dynamically for payload formats defined through non-RTP means. If RTP packets are generated periodically, the nominal sampling instant as determined from the sampling clock is to be used, not a reading of the system clock. The initial value of the timestamp should be random, as for the sequence number. Timestamps of different flows may advance at different rates and have independent random shifts. Therefore, being them sufficient to recover synchronism of a unique flow, the direct comparison between timestamps is not effective for synchronism of different means. However, for each mean the timestamp relates with the sampling instant by pairing of itself with a reference clock which represents the time when the timestamp's corresponding information was sampled.
- **SSRC Identifier:** The SSRC 32-bit field identifies the synchronization source. This identifier should be chosen randomly, with the intent that no two synchronization sources within the same RTP session will have the same SSRC identifier. Although the probability of multiple sources choosing the same identifier is low, all RTP implementations must be prepared to detect and resolve collisions. If a source changes its source transport address, it must also choose a new SSRC identifier to avoid being interpreted as a looped source
- **CSRC Identifier:** 0 to 15 items, 32 bits each. The CSRC list identifies the contributing sources for the payload contained in this packet. The number of identifiers is given by the CC field. If there are more than 15 contributing sources, only 15 can be identified. CSRC identifiers are inserted by mixers, using the SSRC identifiers of contributing sources. For example, for audio



packets the SSRC identifiers of all sources that were mixed together to create a packet are listed, allowing correct talker indication at the receiver.

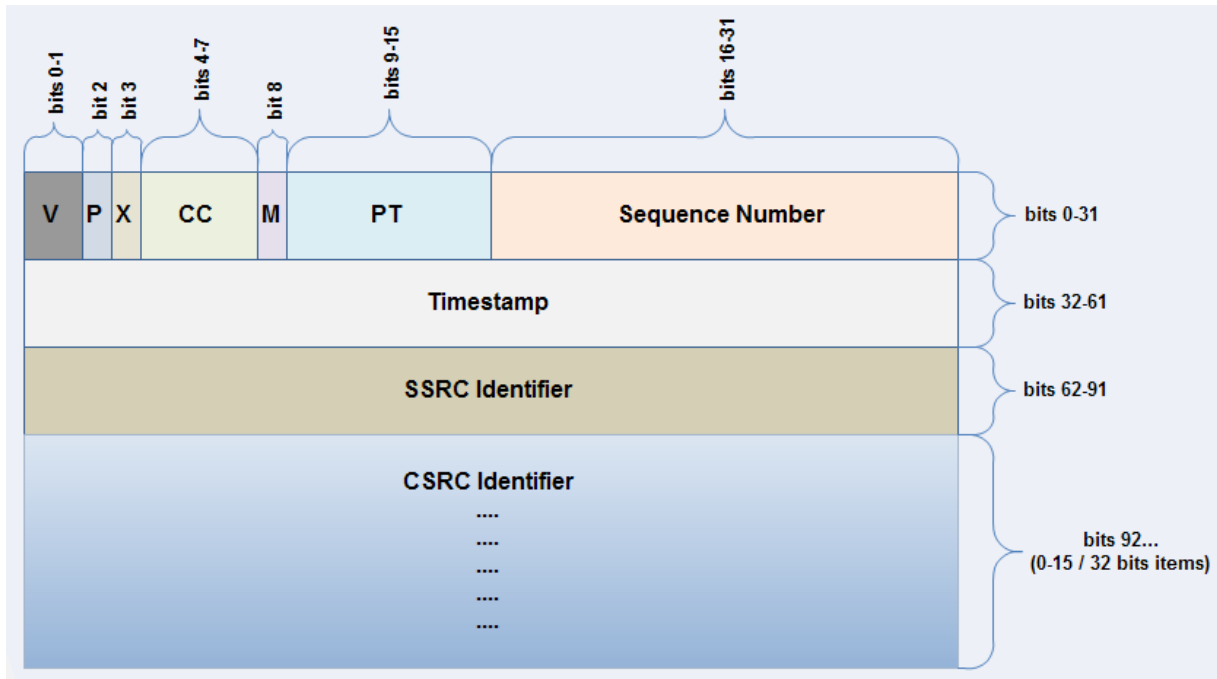


Figure E - 35. RTP Packet header.

#### E.4.2.2 RTP Control Protocol (RTCP)

RTCP is always used with RTP (both specified by IETF RFC 3550). It provides bidirectional information QoS statistics, information for performing inter-media mapping and synchronization between binary dispatch RTP identifiers and human readable names (useful in conferences where the media of all participants is received in the same direction of transport).

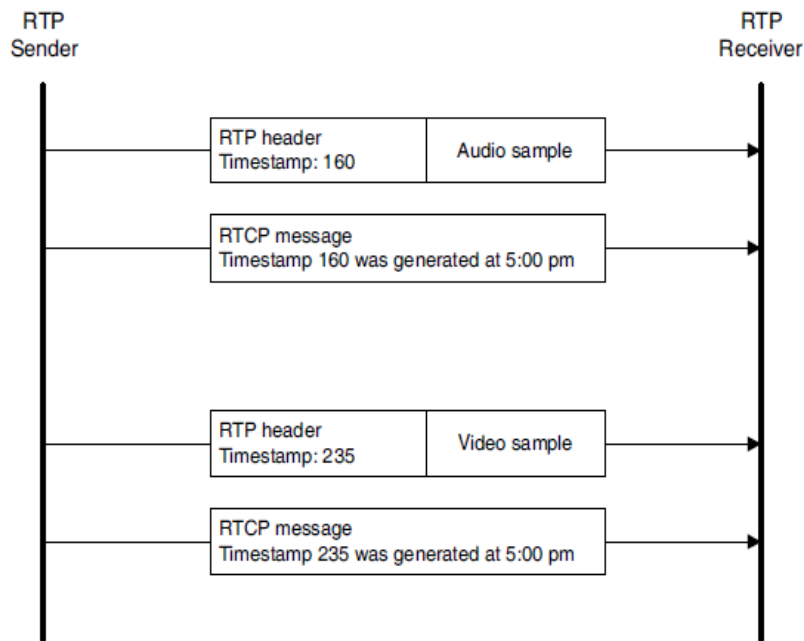


Figure E - 36. This figure shows how RTCP mappings perform inter-media synchronization [34].

Generating QoS statistics (or rate of packet loss during an RTP session) requires that by RTCP, RTP transmitters report the number of packets sent to the network and the number of packets received by the RTP receivers.

For an RTP source, RTCP conveys a persistent identifier at transport level named CNAME («Canonical Name»). Since SSRC identifier may be modified due to a conflict or an application restart, receptors require this CNAME for keeping identifying each participant.

Receivers may also require the CNAME for associating flows from several mediums from a specific participant, for example to synchronize audio and video. Inter-media synchronism also requires NTP and RTP timestamps included by the RTCP originators. Then, RTCP provides mapping between the media flows timestamps and a reference or «wall-clock». Likewise, receivers may synchronize different flow media reproduction.

Since clock frequencies used for timestamps of different media streams can be different and the initial value of the timestamps random, references to a wall-clock are

necessary. Then, only by inspection of the timestamps between two media streams, it is impossible determining which samples should be played at the same time.

When SDP is used, RTP packets are normally sent by an even number port, meanwhile RTCP messages are sent via the subsequent odd port. For example, a session description embedded in SDP within a SIP INVITE message, exposes the reception of RTP packets transporting audio samples over UDP at port 2010 through the following text line: «m=audio 20100 RTP/AVP 0 98». In this case, RTCP messages related to this media stream are received via UDP at port 20101.

#### E.4.2.2.1 RTCP Packet Structure

IETF RFC specification defines several RTCP types of packets for a variety of information transport, namely:

- **Sender Report (SR)**: Report of transmission statistics of either sender or receiver participants that actively transmit during the session.
- **Receiver Report (RP)**: reception statistics from participants that are not active senders and in combination with SR for active senders reporting on more than 31 sources.
- **Source Description (SDES)**: source description items, including CNAME.
- **BYE**: Indicates end of transmission/participation.
- **APP**: Application-specific functions.

Each RTCP packet begins with a fixed part similar to RTP data packets, followed by structured elements that may be of variable length according to the packet type, but must end on a 32-bit boundary. The alignment requirement and a length field in the fixed part of each packet are included to make RTCP packets «stackable». Multiple RTCP packets can be concatenated without any intervening separators to form a compound RTCP packet that is sent in a single packet of the

lower layer protocol (e.g. UDP). There is no explicit count of individual RTCP packets in the compound packet since the lower layer protocols are expected to provide an overall length to determine the end of the compound packet.

It is recommended that translators and mixers combine individual RTCP packets from the multiple sources they are forwarding into one compound packet whenever feasible in order to amortize the packet overhead. An example RTCP compound packet as might be produced by a mixer is shown in next figure. If the overall length of a compound packet would exceed the MTU of the network path, it should be segmented into multiple shorter compound packets to be transmitted in separate packets of the underlying protocol. This does not impair the RTCP bandwidth estimation because each compound packet represents at least one distinct participant. Note that each of the compound packets must begin with an SR or RR packet.

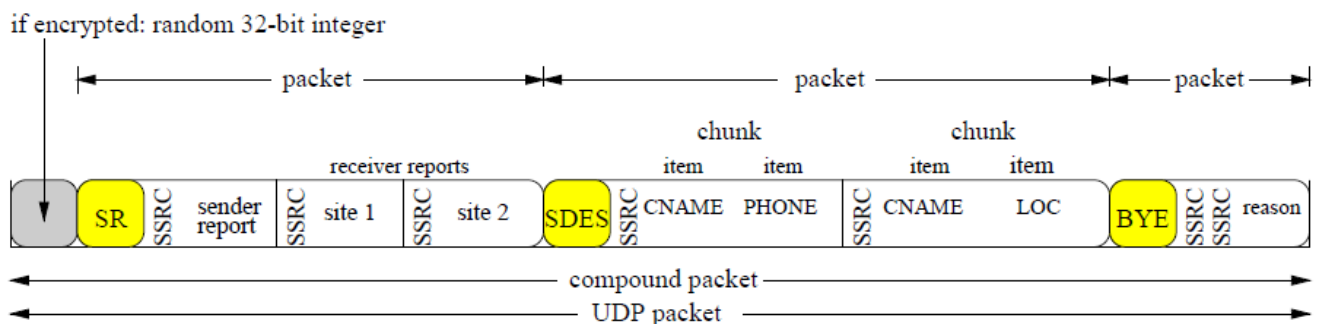


Figure E - 37. RTCP compound packet structure [Source: IETF RFC 3550].

#### E.4.2.3 Security for RTP/RTCP: SRTP

Specified by IETF RFC 3711, SRTP provides confidentiality, authentication and protection of RTP/RTCP traffic duplication.

Peers using SRTP for information exchange use a key management protocol in order to generating a master key, which is used for session key generation. These, are periodically refreshed for security means, so as potential hackers do not have access to big volumes of traffic encrypted under the same key.

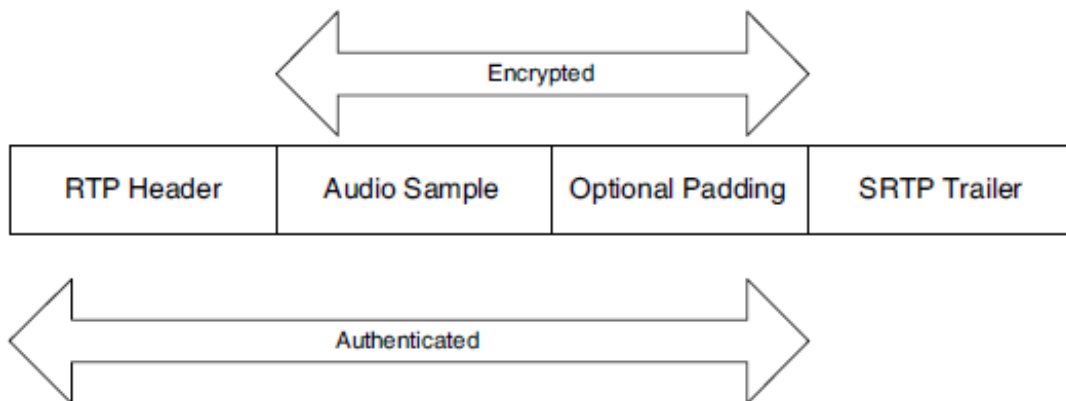


Figure E - 38. Authenticated and encrypted RTP packet sections [34].

## E.5 Brief Introduction to WebRTC

WebRTC is a free open project supported by Ericsson, Google (Chrome), Mozilla Firefox and Opera [136], that enables web browsers with Real-Time Communications (RTC) capabilities via simple JavaScript APIs.

	Classic VoIP	WebRTC
Signaling	Mostly SIP or H.323	Undefined
Media Transport	RTP/RTCP	RTP/RTCP
Security	SRTP for SIP, H.235 for H.323	DTLS-SRTP
NAT traversal	STUN/TURN/ICE for SIP H.450.x for H.323	STUN/TURN/ICE
Video Codecs	H.263, H.264	VP8
Voice Codecs	ITU-T G7xxx series mostly	G.711, iLBC, iSAC, Opus

Table E - 4. Differences between classic VoIP and WebRTC.

WebRTC uses `RTCPeerConnection` to communicate streaming data between browsers, also known as peers. `RTCPeerConnection` is the WebRTC component that handles stable and efficient communication of streaming data between peers.

WebRTC doesn't define the signaling protocol. Thus, it allows using anything for signaling including WebSockets, Ajax, server push or plain HTTP and anything on top of that, SIP, XMPP, proprietary, etc. Media is peer to peer and can handle either audio or video.

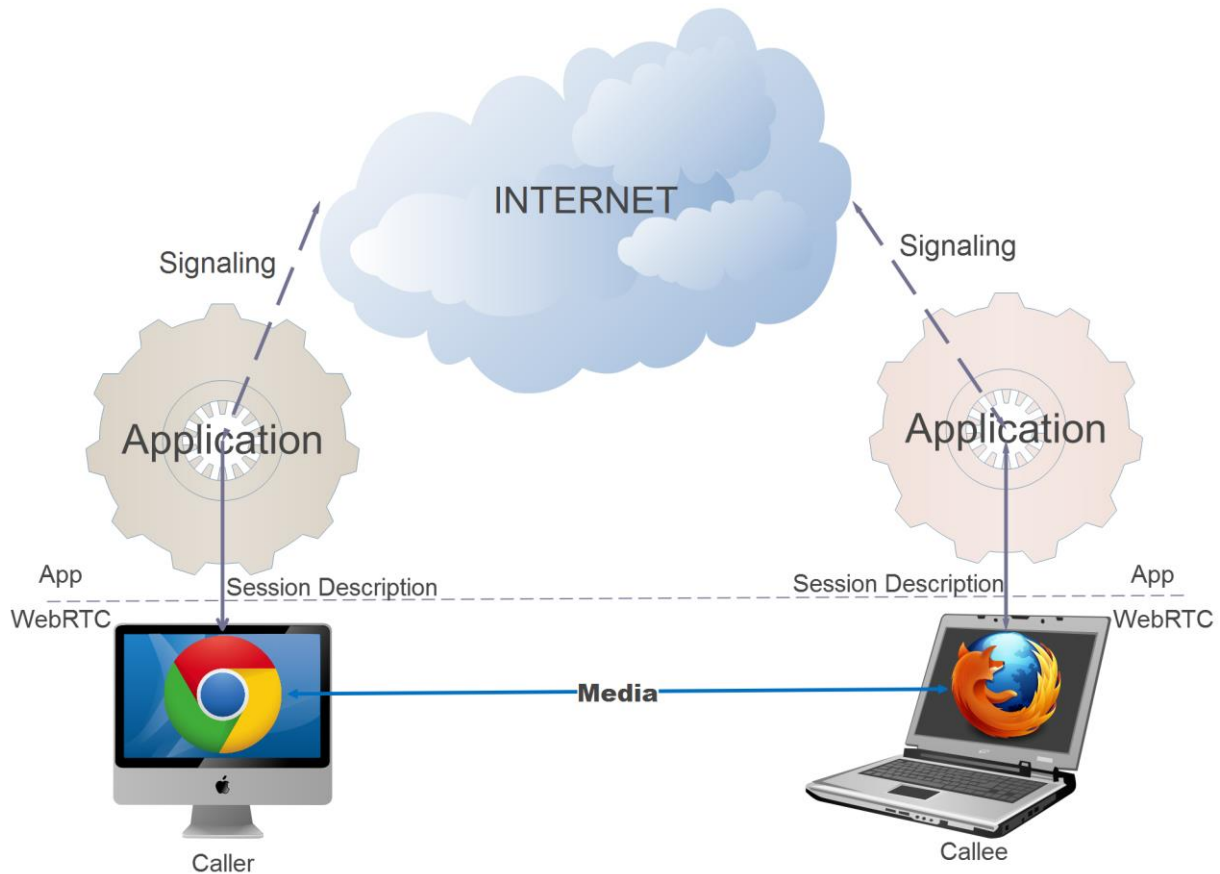


Figure E - 39. WebRTC peer-to-peer communication main components, control and user planes.

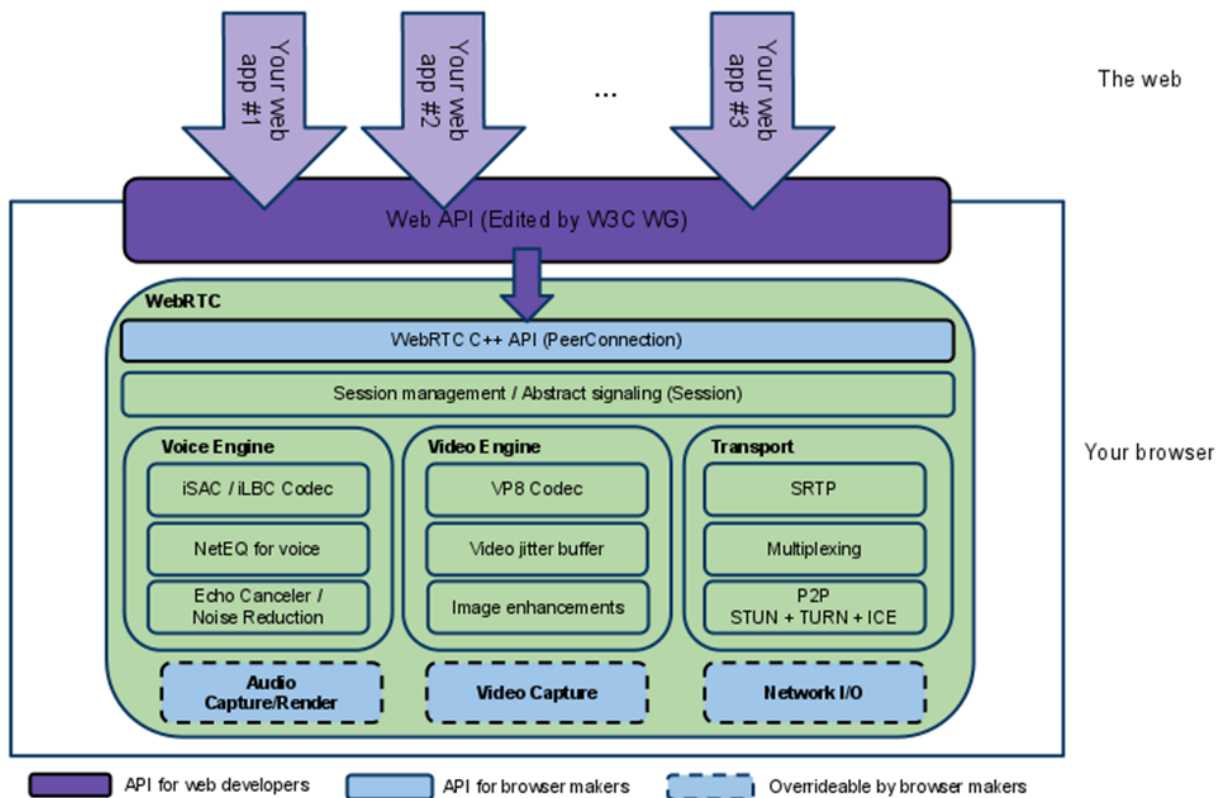


Figure E - 40. WebRTC Architecture.

### E.5.1 SIP over WebSockets for WebRTC

As for IETF RFC 7118 [137] a call is established via SIP after a regular HTTP request with «Upgrade» header. Then, the communication between the browser and the server is not through HTTP anymore, just plain subprotocol except it's masked, thus plaintext cannot be misinterpreted and avoid security issues.

SIP methods/transactions are then carried in WebSocket data new SIP transport: WS or WSS (for secure communication via TLS).

WebSockets endpoints (e.g. mobile phone) need a TCP/TLS connection to be maintained even when not within a call, otherwise they cannot receive calls.

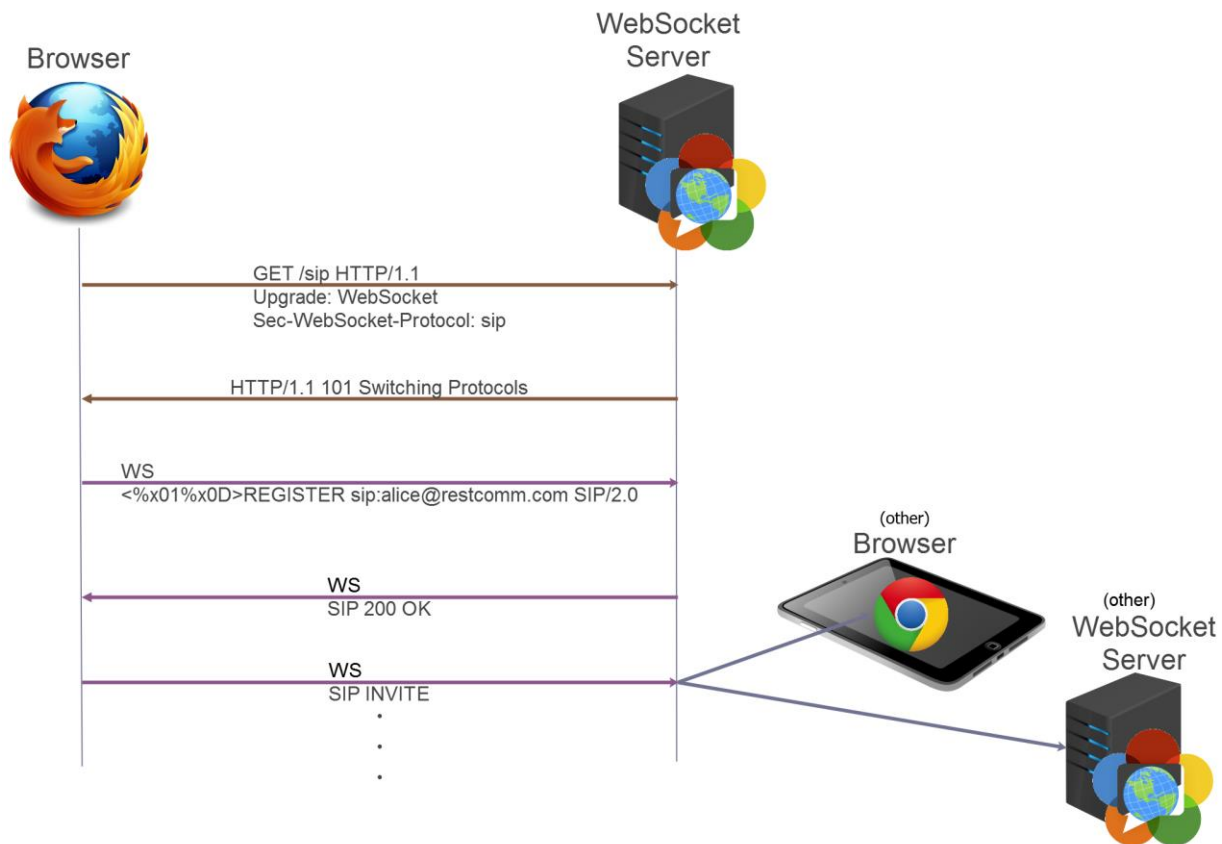


Figure E - 41. WebRTC call establishment via SIP post HTTP WebSocket upgrade.

WebSockets are supported by:

- ✓ Java EE 7.
- ✓ SIP Servlets Specification (JSR 359) support SIP over WebSockets as for latest revision [138].
- ✓ TeleStax SIP Servlets Container since 2012.

RestComm Web, iOS and Android SDKs and client's exposure over RestComm-Connect platform comprise one of the finest Open Source implementations of WebRTC through SIP within WebSockets (refer to figure 3.7 for the first cellular LTE WebRTC video call via RestComm iOS and Android SDKs).



## Annex F

### F Diameter

#### F.1 Introduction to Diameter

A multimedia or IP telephony services network would not be worthwhile without considering security and charging policies. For these purposes Authorization, Authentication and Accounting (AAA) protocols were implemented. As already stated earlier, Diameter is the evolution of the first one of those, RADIUS. Diameter, specified by IETF RFC 6733 [31], consists of a base protocol extended by self-nominated «Diameter extensions», which constitute adaptations or extensions to Diameter in order to fit specific applications within a particular environment. Modern IP-based networks like the IMS or LTE use Diameter in a wide variety of interfaces, even though not all of them use the same Diameter application. For example, the IMS defined a Diameter application together with SIP during session establishment, as well as another way to manage accounting for subscriber credit control. Furthermore, and as has been part of this work, Diameter has been used by 3GPP/LTE to extend multiple mobile core networks capabilities in LTE's EPC previously covered by SS7' MAP in Circuit-Switched core networks like GSM or the UMTS, e.g. SL<sub>h</sub> and SL<sub>g</sub> interfaces for location services in LTE.

#### F.2 Diameter base definitions and generalities

Diameter is a binary format coded protocol specified by IETF RFC 6733 [31]. It is explicitly defined as a base protocol and a set of application for complementing its basics functionalities. Diameter base protocol needs to be implemented in all Diameter nodes, independently of any specific application.

Applications include extensions of the basic functionality and are designed for specific uses of Diameter base protocol in a particular context. The fact that they are extensions allows the development of new applications if necessary. These Diameter applications include features with increasing IP telephony nodes/interfaces, such as adaptations for «Network Access Server» (NAS), credit control, SIP, mobile applications, location services, etc.

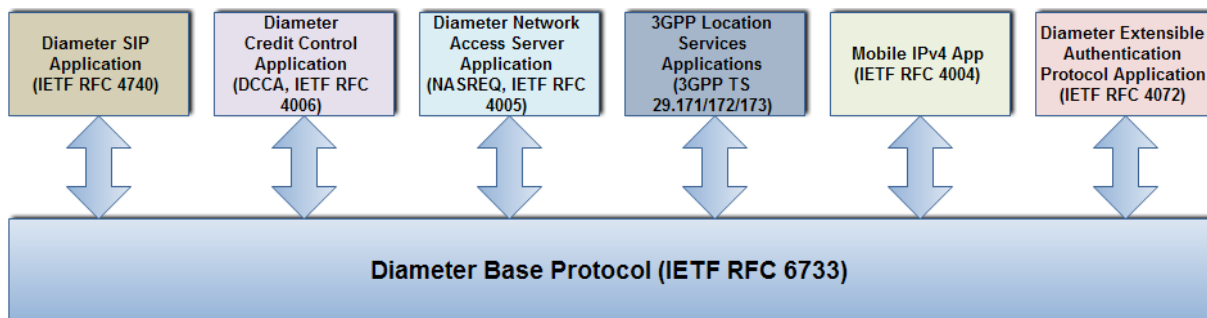


Figure F - 1. Example of Diameter base protocol and some extensions.

## F.2.1 Diameter Transport

Diameter uses reliable transport protocols offering congestion control such as TCP and/or SCTP (on both over port 3868 as assigned by the Internet Assigned Numbers Authority -IANA-). In other words, as opposed to RADIUS from which Diameter evolved, it is not transported on non-reliable transport protocols such as UDP or DCCP. Diameter's transport profile is defined by IETF RFC 3539.

For TLS [IETF RFC 5246] y DTLS (Datagram Transport Layer Security) [IETF RFC 6347], a Diameter node must initiate a connection over port 5868 previous to any message exchange. It is assumed that TLS runs over TCP when used, meanwhile DTLS is used over SCTP. For retro-compatibility with older Diameter nodes as for IETF RFC 3588, in case they cannot receive TLS/TCP or DTLS/SCTP over port 5868, the initiator might revert to use TCP or SCTP over 3868.

Lost Diameter messages are retransmitted on each hop. Moreover, Diameter provides a «heartbeat» message at application level so as to monitoring the state of the connection and allowing its recovery after failures.

Diameter also allows routing credit control messages to alternative servers according to previous authentication/authorization messages.

### F.2.2 Diameter Functional Entities

Diameter is not a typical client/server type of protocol but a «peer-to-peer» communication protocol. Hence, every Diameter node can send a request to its peer. Opposed to what happens with client/server protocols like SIP, neither the «Diameter client» node does comprise a functional entity responding to a request nor does the «Diameter Server» node comprise a functionality entity placed only to reply incoming requests. Instead, both of them can send requests and responses to each other. The «Diameter client» node performs access control meanwhile the «Diameter Server» node is the entity that carries out authentication and authorization.

Diameter messages are either requests or responses. A request is replied by an only response. With rare exceptions, Diameter requests are always answered. Thus, in case of failure or error, the transmitter can easily retrieve a particular state based on relevant received information related to the purpose of the request.

Diameter base protocol defines functional entities for AAA functionalities, namely:

- **Diameter Client.** Functional entity normally placed at the edge of a network for access control. Examples of this entity are NAS («Network Access Servers») and Mobile IP FA («Mobile IP Foreign Agents»).
- **Diameter Server.** Functional entity in charge of AAA functions for a particular domain. It supports server applications over the base protocol, as it should support TCP or SCTP connections.

- **Realm.** Correspond to an administrative domain related to the character string following the «@» in the NAI field («Network Address Indicator», IETF RFC 4282), used by Diameter for retrieving identity and user domain information during the authentication and/or authorization process meanwhile it is used with sole routing purposes. NAI domain names are needed unique and overlapped in the DNS administration space. Diameter makes use of the realm, also referred as domain, in order to determine if messages might be successfully processed locally or if the need to be rerouted or redirected.
  - Home Realm. It corresponds to the domain to which the user keeps an accounting relationship.
  - Local Realm. It corresponds to the administrative domain that provides services to a user. It might act as «Local Realm» for some users as «Home Realm» for others.
- **Proxy.** Functional entity primarily responsible for forwarding Diameter messages. Additionally, it may modify them based on a set of policies that derive decisions related to use of resources, admission control and provisioning. Typically, this is done via state tracking of NAS devices. While proxies usually do not respond to client requests prior to receiving messages from a server, they can reject messages in cases where policies are violated (for which they need to understand the semantics of all messages that pass through them, and not always support all applications).
- **Relay.** Functional entity that forwards Diameter messages based on routing information and routing domain table entries. A relay is typically transparent during the communication. It may modify Diameter messages only through insertion or removal of routing related data, but it may not change any other type of information contained in the message. They do not keep state of sessions or NAS resources.
- **Redirect Agent.** Functional entity that refers clients to servers and allow them to communicate directly. They do not alter any AVP (Attribute Value Pair) between client/server, given they are not located in the forwarding path. They do not origin messages and support any type of messages even

though they can only be configured for redirecting certain type of messages, meanwhile acting as relay or proxy for other types. They do not keep state of sessions or NAS resources.

- **Translation Agent.** Functional entity that performs translation between Diameter and other AAA protocols such as RADIUS.
- **Diameter Node.** Functional entity which implements Diameter protocol and acts either as Diameter Client, Diameter Server, Proxy, Relay, Redirect Agent or Translation Agent.

### F.2.3 Diameter Resource Identifiers

AAA protocols like Diameter are enabled to use «aaa» or «aaas» URI for identifying resources. The syntax of these URIs are like shown next (FQDN: Fully Qualified Domain Name):

```
"aaa://" FQDN [ port ] [ transport ] [ protocol ]
```

```
"aaas://" FQDN [ port ] [ transport ] [ protocol ]
```

URIs may contain a port number, transport protocol and AAA options to access the desired resource. The port by default is assumed in case it is absent (3868 for Diameter). The transport by default is SCTP for Diameter. The default protocol is Diameter. «aaa» or «aaas» URI examples are shown next

```
aaas://host.ex.net
```

```
aaa://host.ex.org:5658;transport=tcp;protocol=diameter
```

```
aaa://accserver.ex.net:1813;transport=udp;protocol=radius
```

```
aaa://server.ex.net:49;transport=tcp;protocol=tacacs+
```

```
aaa://aaaserver.ex.net
```

## F.2.4 Diameter Connections and Sessions

A Diameter connection refers to a transport-level connection between two peers that is used to send and receive Diameter messages.

Analogue to multimedia sessions in the control plane based on SIP/SDP, Diameter specification also addresses the session concept but with a wider approach. According to IETF RFC 6733 [31], a Diameter session is a logical concept involving the sequence of events related to a specific activity at the application layer that exists between the Diameter client and the Diameter server; it is identified via the Session-Id AVP. Diameter application documentation provide the guidelines for starting and ending sessions.

Examples of a Diameter session are detailed next:

- ✓ Within the context of a user that dials towards a NAS, the session is composed of all Diameter messages exchanged between the NAS and the Diameter server since the moment the user dials-up until the connection is interrupted.
- ✓ In the IMS context, a Diameter session might be composed of all messages exchanged between a SIP proxy or S-CSCF (acting as Diameter Client) and the HSS (acting as Diameter Server) during the time when the user is registered at the S-CSCF.

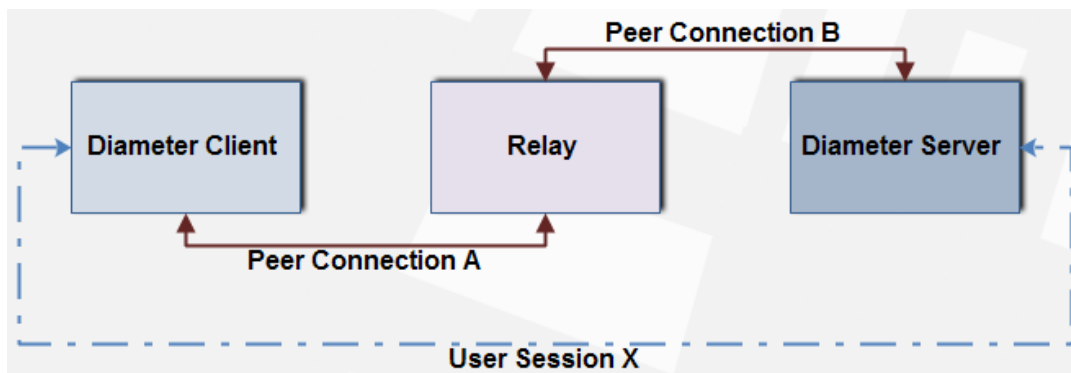


Figure F - 2. Diameter Connections and Sessions.

Each user of a service causes an authorization request to be sent with a univocal identification session. Once accepted by the server, both the server and the client are aware of the session established between them, beyond the connections between intermediate pairs.

It is important to note that there is no relationship between connection and session, meanwhile Diameter messages for multiple sessions are all multiplexed through a single connection. Also, note that messages belonging to a session, either the application specific or the Diameter base protocol, must carry the application identifier or «Application ID». Messages belonging to the establishment and maintenance of connection between peers transport the application identifier set to zero or «Application-Id=0».

### F.3 Diameter message structure

A Diameter message consists of a 20 octets header and a variable amount of data containers named as AVP («Attribute-Value Pairs»). The amount of AVP depend on the Diameter message; they typically include AAA data. The Diameter message structure is divided in the fields described next:

- **Version.** This Version field must be set to 1 to indicate Diameter Version 1.
- **Message length.** The Message Length field is three octets and indicates the length of the Diameter message including the header fields and the added AVPs. Thus, the Message Length field is always a multiple of 4.
- **Command Flags.** The Command Flags field is eight bits. The following bits are assigned:

0	1	2	3	4	5	6	7
R	P	E	T	r	r	r	r

- **R (Request):** If set, the message is a request. If cleared, the message is an answer.

- **P (Proxiable)**: If set, the message may be proxied, relayed, or redirected. If cleared, the message must be locally processed.
  - **E (Error)**: If set, the message contains a protocol error, and the message will not conform to the CCF described for this command. Messages with the 'E' bit set are commonly referred to as error messages. This bit **MUST NOT** be set in request messages.
  - **T (Potentially retransmitted message)**: This flag is set after a link failover procedure, to aid the removal of duplicate requests. It is set when resending requests not yet acknowledged, as an indication of a possible duplicate due to a link failure. This bit must be cleared when sending a request for the first time; otherwise, the sender must set this flag. Diameter agents only need to be concerned about the number of requests they send based on a single received request; retransmissions by other entities need not be tracked. Diameter agents that receive a request with the T flag set, must keep the T flag set in the forwarded request. This flag must not be set if an error answer message (e.g., a protocol error) has been received for the earlier message. It can be set only in cases where no answer has been received from the server for a request, and the request has been sent again. This flag must not be set in answer messages.
  - **r (reserved)**: these bits are reserved for future use and must be set to 0 and ignored by the receiver.
- **Command Code**. The Command Code field is three octets and is used in order to communicate the command associated with the message. The 24-bit address space is managed by IANA. Command Code values 16.777.214 and 16.777.215 (hexadecimal values FFFFFE and FFFFFFF) are reserved for experimental use.
  - **Application-ID**. Application-ID is four octets long and is used to identify for which application the message is applicable. The application can be an authentication application, an accounting application, or a vendor-specific



application. The value of the Application-ID field in the header must be the same as any relevant Application-Id AVPs contained in the message.

- **Hop-by-Hop Identifier.** The Hop-by-Hop Identifier is an unsigned 32-bit integer field (in network byte order) that aids in matching requests and replies. The sender must ensure that the Hop-by-Hop Identifier in a request is unique on a given connection at any given time, and it may attempt to ensure that the number is unique across reboots. The sender of an answer message **MUST** ensure that the Hop-by-Hop Identifier field contains the same value that was found in the corresponding request. The Hop-by-Hop Identifier is normally a monotonically increasing number, whose start value was randomly generated. An answer message that is received with an unknown Hop-by-Hop Identifier **MUST** be discarded.
- **End-to-End Identifier.** The End-to-End Identifier is an unsigned 32-bit integer field (in network byte order) that is used to detect duplicate messages. Upon reboot, implementations **MAY** set the high order 12 bits to contain the low order 12 bits of current time, and the low order 20 bits to a random value. Senders of request messages must insert a unique identifier on each message. The identifier must remain locally unique for a period of at least 4 minutes, even across reboots. The originator of an answer message must ensure that the End-to-End Identifier field contains the same value that was found in the corresponding request. The End-to-End Identifier must not be modified by Diameter agents of any kind. The combination of the Origin-Host AVP (Section 6.3) and this field is used to detect duplicates. Duplicate requests **SHOULD** cause the same answer to be transmitted (modulo the Hop-by-Hop Identifier field and any routing AVPs that may be present), and they must not affect any state that was set when the original request was processed. Duplicate answer messages that are to be locally consumed should be silently discarded.
- **AVPs.** AVPs are a method of encapsulating information relevant to the Diameter message.

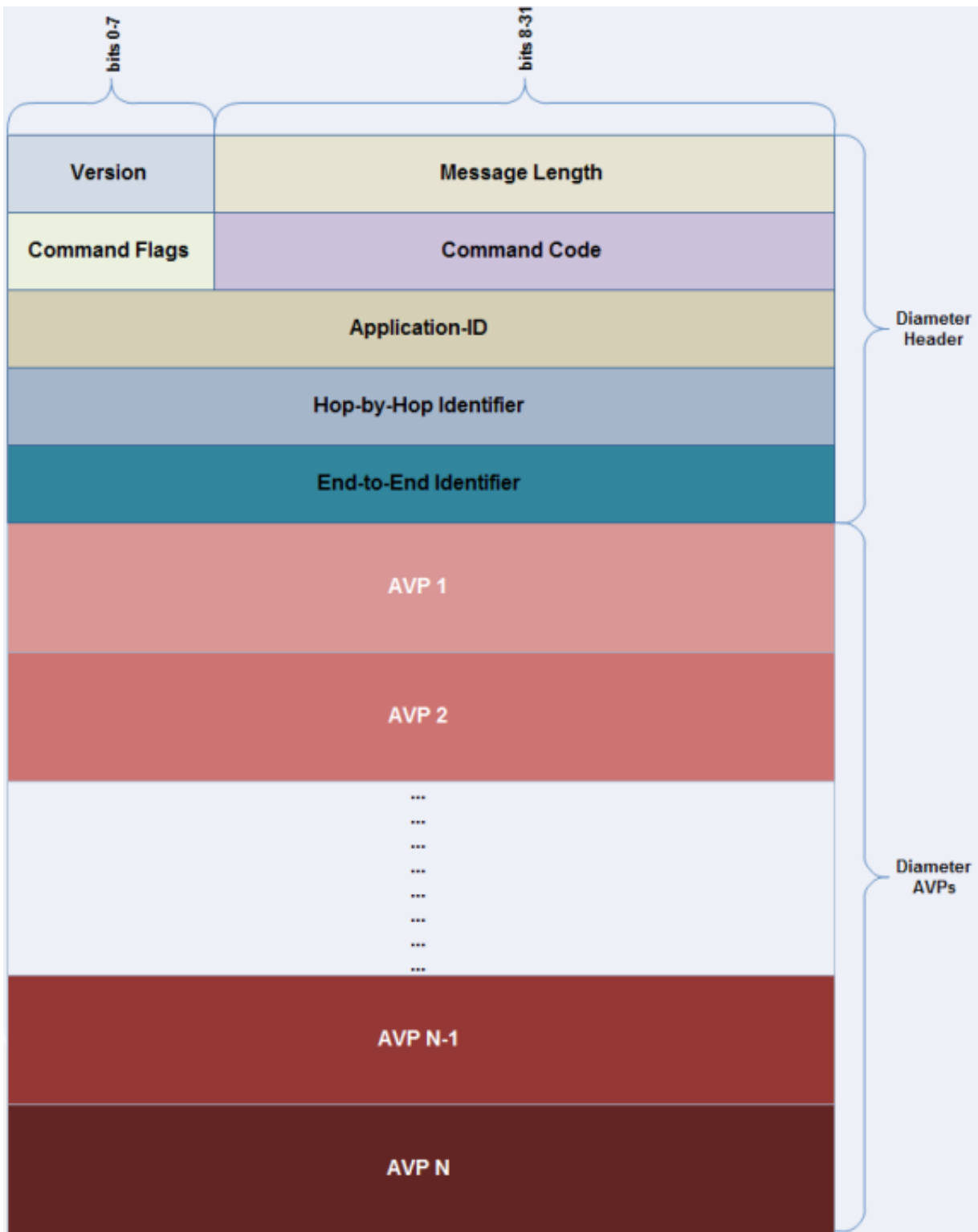


Figure F - 3. Diameter message structure.

### F.3.1 Diameter AVP structure

AVPs encapsulate information relevant to Diameter messages. Diameter AVPs carry specific authentication, accounting, authorization, and routing information as well as configuration details for the request and reply. The fields in the AVP header MUST be sent in network byte order. Next figure shows the structure of Diameter AVPs.

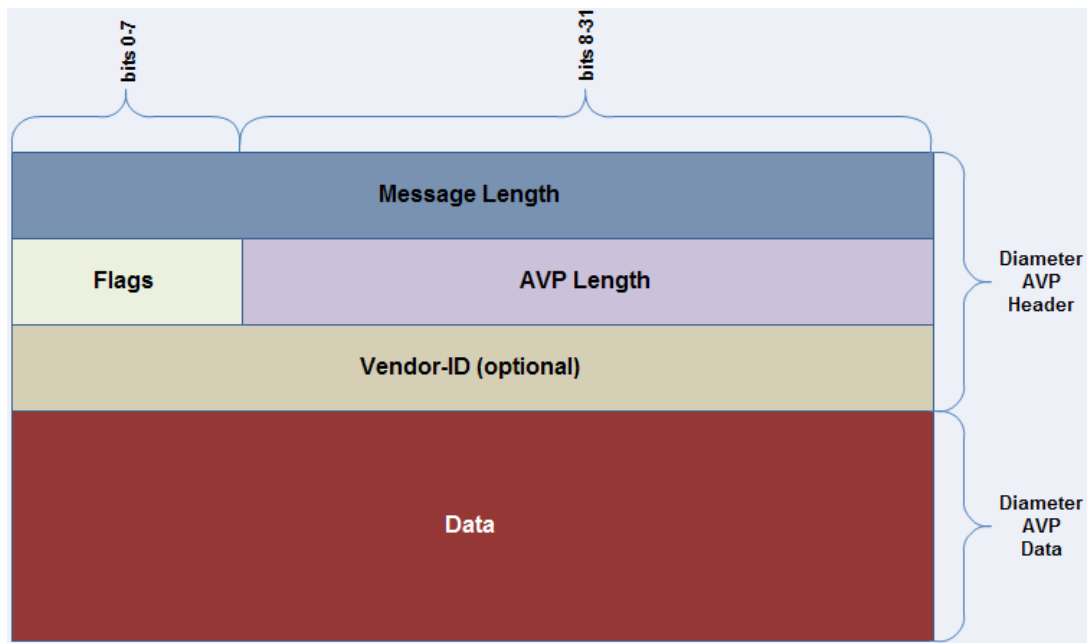
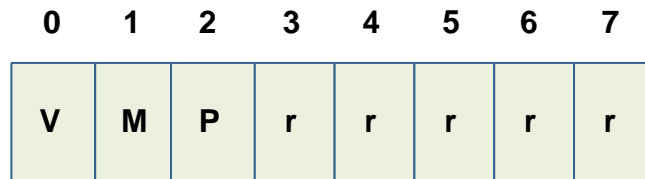


Figure F - 4. Diameter AVP structure.

AVP fields are described next:

- **AVP Code.** The AVP Code, combined with the Vendor-Id field, identifies the attribute uniquely. AVP numbers 1 through 255 are reserved for reuse of RADIUS attributes, without setting the Vendor-Id field. AVP numbers 256 and above are used for Diameter, which are allocated by IANA.
- **AVP Flags.** The AVP Flags field informs the receiver how each attribute must be handled. New Diameter applications should not define

additional AVP Flag bits. However, note that new Diameter applications may define additional bits within the AVP header, and an unrecognized bit should be considered an error.



- **V (Vendor)**: known as the Vendor-Specific bit, indicates whether the optional Vendor-ID field is present in the AVP header. When set, the AVP Code belongs to the specific vendor code address space.
- **M (Mandatory)**: indicates whether the receiver of the AVP must parse and understand the semantics of the AVP including its content. The receiving entity must return an appropriate error message if it receives an AVP that has the M-bit set but does not understand it. An exception applies when the AVP is embedded within a Grouped AVP or if the AVP arrives from a Diameter Relay or Redirect node. The «M» bit must be set according to the rules defined in the application specification that introduces or reuses this AVP. Within a given application, the M-bit setting for an AVP is defined either for all command types or for each command type. AVPs with the «M» bit cleared are informational only. Receiver not supporting the AVP value may simply ignore it.
- **P**: The «P» bit has been reserved for future usage of end-to-end security. As for [31] there are no end-to-end security mechanisms specified; therefore, the «P» bit should be set to 0
- **r (reserved)**: The sender of the AVP must set «r» bits to 0 and the receiver should ignore all «r» bits.
- **AVP Length**. The AVP Length field is three octets, and indicates the number of octets including the AVP Code field, AVP Length field, AVP

Flags field, Vendor-ID field (if present), and the AVP Data field. If a message is received with an invalid attribute length, the message must be rejected.

- **Vendor-ID** (optional). The Vendor-ID field is present if the «V» bit is set in the AVP Flags field. The optional four-octet Vendor-ID field contains the IANA-assigned «SMI Network Management Private Enterprise Codes» [ENTERPRISE] value, encoded in network byte order. Any vendors or standardization organizations that are also treated like vendors in the IANA-managed «SMI Network Management Private Enterprise Codes» space wishing to implement a vendor-specific Diameter AVP must use their own Vendor-ID along with their privately managed AVP address space, guaranteeing that they will not collide with any other vendor's vendor-specific AVP(s) or with future IETF AVPs. A Vendor-ID value of zero (0) corresponds to the IETF-adopted AVP values, as managed by IANA. Since the absence of the Vendor-ID field implies that the AVP in question is not vendor specific, implementations must not use the value of zero (0) for the Vendor-ID field. The combination of this field along with Product-name y Firmware-Revision can be useful for debugging errors.
- **Data** (optional). Includes the information specific to the AVP. It contains zero or more octets, as indicated by the «AVP Length» field. The Diameter base protocol specifies different formats for this field, namely: OctetString, Integer32, Integer64, Unsigned32, Unsigned64, Float32, Float64 and Grouped. Applications may define data formats derived from the Basic AVP data formats. The Diameter base protocol already defines some AVP formats, being the most important the ones depicted next:
  - Address: used for conveying an IPv4 or IPv6 address.
  - Time: used for date and time presentation.
  - UTF8String: used for representing a character string coded in UTF8 format.
  - DiameterIdentity: is used to uniquely identify either a Diameter node for purposes of duplicate connection and routing loop

- detection, or a Realm to determine whether messages can be satisfied locally or whether they must be routed or redirected.
- DiameterURI: used to communicate either an «aaa» or «aaas» URI.
  - Enumerated: numeric value that represent some semantics.
  - Result-Code: indicates if the request was completed successfully or not (conveyed in all responses).
  - Origin-Host: transmits the complete realm name generator of the request generator Diameter node (client).
  - Origin-Realm: includes the Originating Diameter node realm.
  - Destination-Host: transmits the complete realm name generator of the request destination Diameter node (server).
  - Destination-Realm: used when the user does not know the current name of the server but the administrative domain where its user name is valid or defined. It is always included for those requests that may be routed through proxies to the destination domain.
  - Authorization-Lifetime: indicates the time period by which an user authorization is valid.

## F.4 Diameter base protocol commands

As described in previous sections, Diameter messages compose requests and responses. The «R» bit of the «Command Flags» header field indicates whether if the command is a request or its corresponding response. A request and its corresponding response are identified by the «Command Code» header field, which comprises an identifier number for the action to be taken in the server node, destination of the request. This number is identical either for request as for its response, therefore the need of the «R» bit.

Diameter base protocol as for IETF RFC 6733 [31] specifies an initial amount of «Command Code» values. As stated earlier, an application may extend these basic commands and add its specific ones. The next table shows the request/response messages defined by the Diameter base protocol.

Command name	Acronym	«Command Code»	Type
Abort-Session-Request	ASR	274	Authentication, Authorization
Abort-Session-Answer	ASA	274	Authentication, Authorization
Accounting-Request	ACR	271	Accounting
Accounting-Answer	ACA	271	Accounting
Capabilities-Exchange-Request	CER	275	Authentication, Authorization
Capabilities-Exchange-Answer	CEA	275	Authentication, Authorization
Device-Watchdog-Request	DWR	280	Authentication, Authorization
Device-Watchdog-Answer	DWA	280	Authentication, Authorization
Disconnect-Peer-Request	DPR	282	Authentication, Authorization
Disconnect-Peer-Answer	DPA	282	Authentication, Authorization
Re-Auth-Request	RAR	258	Authentication, Authorization
Re-Auth-Answer	RAA	258	Authentication, Authorization
Session-Termination-Request	STR	275	Authentication, Authorization
Session-Termination-Answer	STA	275	Authentication, Authorization

Table F - 1. Diameter base protocol commands.

Diameter base protocol commands are briefly described in following subsections.

#### F.4.1 Abort-Session-Request / Abort-Session-Answer (ASR/ASA)

Multiple circumstances may determine that a Diameter Server needs to stop a service provided to a particular user, e.g. the emergence of new needs not foreseen when authentication/authorization of the Diameter session, insufficient credit, security reasons, new administrative orders, etc., which determines aborting a service currently being provided to the user.

When it becomes urgent to Diameter Server to stop a service being provided to a user, it sends an ASR message to the corresponding the Diameter Client, which reports back the execution of the command by replying via an ASA message.

#### F.4.2 Device-Watchdog-Request / Device-Watchdog-Answer (DWR/DWA)

In order to react as soon as possible and carry out the corresponding corrective actions, it is essential for Diameter to be enabled for detecting failures at

application and transport layer. The mechanism provided by Diameter for detecting these incidents is based on an application layer overseer or «watchdog».

Durant traffic periods between Diameter nodes, if one of them sends a request which is not replied within a specific time span, it is considered sufficient for detecting a failure at either application or transport layer. However, during traffic absence periods it is impossible to detect these network failures. The solution for this problem implemented by Diameter consists in conveying DWR messages and its corresponding DWR reply between nodes. The absence of a DWA reply is considered enough to detect a failure in the communication at either application or transport layer.

#### **F.4.3 Disconnect-Peer-Request/Disconnect-Peer-Answer (DPR/DPA)**

A Diameter that has established a transport connection with a Diameter peer could need to close the connection, for instance if it does not foresee further traffic to be exchanged between them. In this case, a DPR message is conveyed to the peer node for indicating the imminent disconnection at transport layer.

The DPR command also transfers the needed semantic for requesting the peer node for not trying to establish a connection unless it is ultimately needed (e.g. to forward a message).

#### **F.4.4 Accounting-Request / Accounting-Answer (ACR/ACA)**

A Diameter node might need to report accounting events to a Diameter Server providing chargeable services. For this regard, Diameter provides the ACR command through which a Diameter client sends reports concerning the usage of a service to a Diameter Server.

The ACR command includes information that allows the Diameter Server registering the beginning and end of a service, as well as accounting events at specific instants.



#### **F.4.5 Capabilities-Exchange-Request/Answer (CER/CEA)**

Once a transport connection is established, first Diameter messages exchanged between peers are CER and CEA. These messages transport the node identity and its capabilities (protocol version, supported Diameter applications, supported security mechanisms, etc.).

#### **F.4.6 Re-Authentication-Request/Answer (RAR/RAA)**

At any time, but especially during long time sessions, the Diameter Server might request a user re-authentication, for the sole purpose of avoiding an eventual hack or fraud. For this concern, a Diameter Server sends RAR command to the Diameter Client, which in turn replies with the corresponding RAA.

#### **F.4.7 Session-Termination-Request/Answer (STR/STA)**

With the aim of indicating the end of a specific service usage, the Diameter Client node reports the fact via a STR command to the Diameter Server, which in turn replies with the corresponding STA.

### **F.5 Diameter in the IMS and LTE**

Basic Diameter interfaces in the IMS will be listed here. Firstly, for authentication and authorization, the following interfaces are defined in the IMS:

- **Cx**: specified between either an I-CSCF or an S-CSCF and an HSS.
- **Dx**: specified between either an I-CSCF or an S-CSCF and an SLF.
- **Sh**: specified between either an SIP-AS or an OSA-SCS and an HSS.
- **Zh**: specified between an HSS and a BSF.
- **Zn**: specified between a BSF and a NAF.

For Accounting, Policy and Charging Control (PCC) in the IMS, the following Diameter interfaces are defined:

- **Rx**: specified between an AF and a PCRF.
- **Gx**: specified between a PCRF and a PCEF.
- **Gz**: specified between the PCEF and the OFCS
- **Ro**: specified between the OCF and any of the following: IMS-GWF, SIP-AS, MRFC or GGSN.
- **Rf**: specified between the CDF and any of the following: MRFC, MGCF, BGCF, SIP-AS, P-CSCF, I-CSCF or S-CSCF.

For other purposes, the following Diameter interfaces are specified between LTE's EPC and IMS:

- **S6a**: specified between an MME and the HSS.
- **SLs**: specified between an MME and the E-SMLC
- **SLg**: specified between an MME and a GMLC.
- **SLh**: specified between an HSS and a GMLC.
- **S13**: specified between an MME and an EIR.

Regardless that most of them have been already covered up to this point in this document, a list of acronyms covering the aforementioned interfaces are listed next:

- **I-CSCF** and **S-CSCF**: Interrogating and Serving Call Session Control Function.
- **HSS**: Home Subscriber Server.
- **SLF**: Subscriber Location Function
- **SIP-AS**: Session Initiation Protocol - Application Server.
- **OSA-SCS**: Open Service Access – Service Capability Server.
- **BSF**: Bootstrapping Server Functionality.
- **NAF**: Network Application Function (operator-controlled functionality)
- **AF**: Application Function (e.g.: SIP-AS, P-CSCF, etc.).
- **PCRF**: Policy and Charging Rules Function.
- **P-CSCF**: Proxy Call Session Control Function.
- **PCEF**: Policy and Charging Enforcement Function
- **OCF**: Online Charging Function.
- **IMS-GWF**: IMS Gateway Function.

- **MRFC**: Media Resource Function Controller.
- **GGSN**: GPRS Gateway Support Node.
- **OFCS**: Offline Charging System.
- **MGCF**: Media Gateway Control Function.
- **BGCF**: Breakout Gateway Control Functions.
- **EPC**: Evolved Packet Core.
- **MME**: Mobility Management Entity.
- **E-SMLC**: Evolved Serving Mobile Location Center.
- **GMLC**: Gateway Mobile Location Center.
- **EIR**: Equipment Identity Register.

For more details on Diameter interfaces and updates between the IMS and LTE, refer to 3GPP TS 23.002 and its internal references regarding Diameter interfaces, i.e.:

3GPP TS 29.272: "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol".

3GPP TS 29.173: "Location Services (LCS); Diameter-based SLh interface for Control Plane LCS".

3GPP TS 29.336: "Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications".

3GPP TS 29.337: "Diameter based T4 Interface for communications with packet data networks and applications".

3GPP TS 29.338: "Diameter based protocols to support of SMS capable MMEs".

IETF RFC 4006: "Diameter Credit-Control Application".

### **F.5.1 Authentication and Authorization in the IMS**

Following table portrays the Diameter commands defined for the Cx interface.

Command Name	Acronym	«Command Code»	Type
User-Authorization-Request	UAR	300	Authentication, Authorization
User-Authorization-Answer	UAA	300	Authentication, Authorization
Server-Assignment-Request	SAR	301	Authentication, Authorization
Server-Assignment- Answer	SAA	301	Authentication, Authorization
Location-Info-Request	LIR	302	Authentication, Authorization
Location-Info-Answer	LIA	302	Authentication, Authorization
Multimedia-Auth-Request	MAR	303	Authentication, Authorization
Multimedia-Auth-Answer	MAA	303	Authentication, Authorization
Registration-Termination-Request	RAR	304	Authentication, Authorization
Registration-Termination-Answer	RAA	304	Authentication, Authorization
Push-Profile-Request	PPR	305	Authentication, Authorization
Push-Profile-Answer	PPA	305	Authentication, Authorization

Table F - 2. Diameter commands for authentication and authorization in the IMS.

Commands outlined in previous table are described in next subsections.

#### **F.5.1.1 User-Authorization-Request/Answer (UAR/UAA)**

An I-CSCF sends a UAR when it receives a SIP REGISTER from an IMS terminal for one of the following reasons:

- ✓ The HSS firstly filters/legitimizes the public user identity in the SIP REGISTER request.
- ✓ The HSS verifies that the subscriber's origin network has a roaming agreement with the network where the P-CSCF is operating. This allows the latter's

network to exchange Call Detail Records (CDRs) with the subscriber's origin network.

- ✓ An I-CSCF needs to determine if an S-CSCF has already been assigned for the public user identity under registration previous to the sending of the SIP REGISTER request from the I-CSCF to the P-CSCF. In case there's no S-CSCF assigned, the I-CSCF shall receive a capabilities set required by the S-CSCF so that the I-CSCF is enabled to select an appropriate S-CSCF.
- ✓ The SIP REGISTER request typically carries the user's private and public identities. The HSS checks that the public identity is allowed to use the private identity for authentication purposes.

#### **F.5.1.2 Multimedia-Auth-Request/Answer (MAR/MAA)**

When an S-CSCF receives an initial SIP REGISTER request, it needs to authenticate the IMS user. Anyway, at the first register request, the S-CSCF does not have authentication vectors, rather they are stored at the HSS. The S-CSCF sends a MAR command to the HSS for obtaining the authentication vectors.

Additionally, the S-CSCF registers its own SIP URI in the user's related data stored in the HSS, so that other CSCF or ASs become enabled for obtaining the URI from the S-CSCF assigned for the particular user through a later interrogation to the HSS.

#### **F.5.1.3 Server-Assignment-Request/Answer (SAR/SAA)**

When the S-CSCF eventually authenticates the user through the private identity, the public user identity is registered and linked to a contact address. At that moment, the S-CSCF sends a SAR command to the HSS for informing that the user is appropriately registered at the S-CSCF. The S-CSCF also requests the user profile associated with the user.

The HSS includes the user's profile in the reply back via a SAA command.

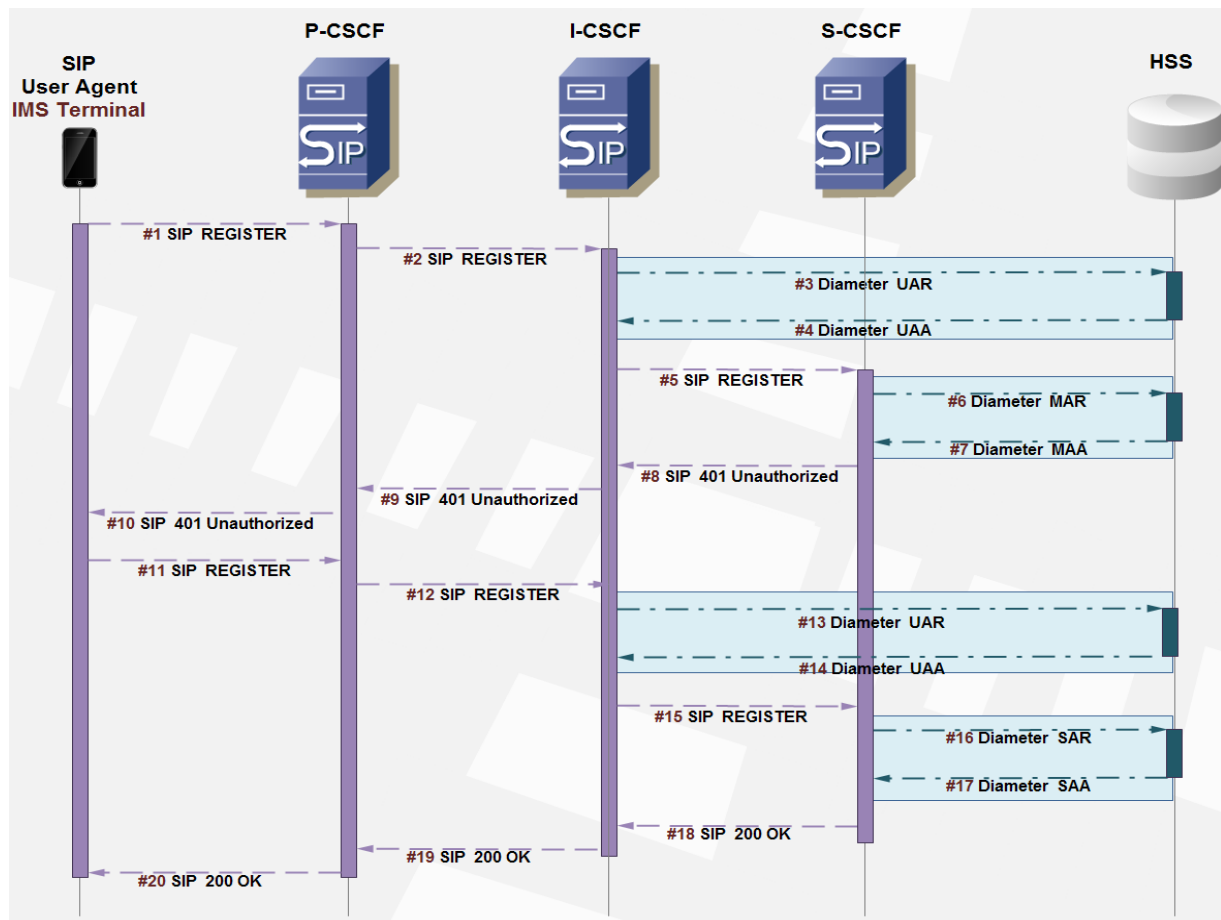


Figure F - 5. Authentication and Authorization in the IMS on first SIP REGISTER.

#### F.5.1.4 Location Information Request/Answer (LIR/LIA)

An I-CSCF receiving a SIP request not containing the header field «Route» pointing to the next SIP hop (S-CSCF), needs to know which S-CSCF is assigned to the user (if there is one). In this context, the I-CSCF sends a LIR command to the HSS.

The HSS responds the LIR with the corresponding LIA, which indicated the SIP URI of the S-CSCF assigned to the user. The next figure illustrates this. In case there isn't a proxy assigned to the user, the HSS shall include the capabilities set required by the S-CSCF so as it is possible for the I-CSCF to choose a S-CSCF for this user (similarly to the selection that takes place during the initial registration).

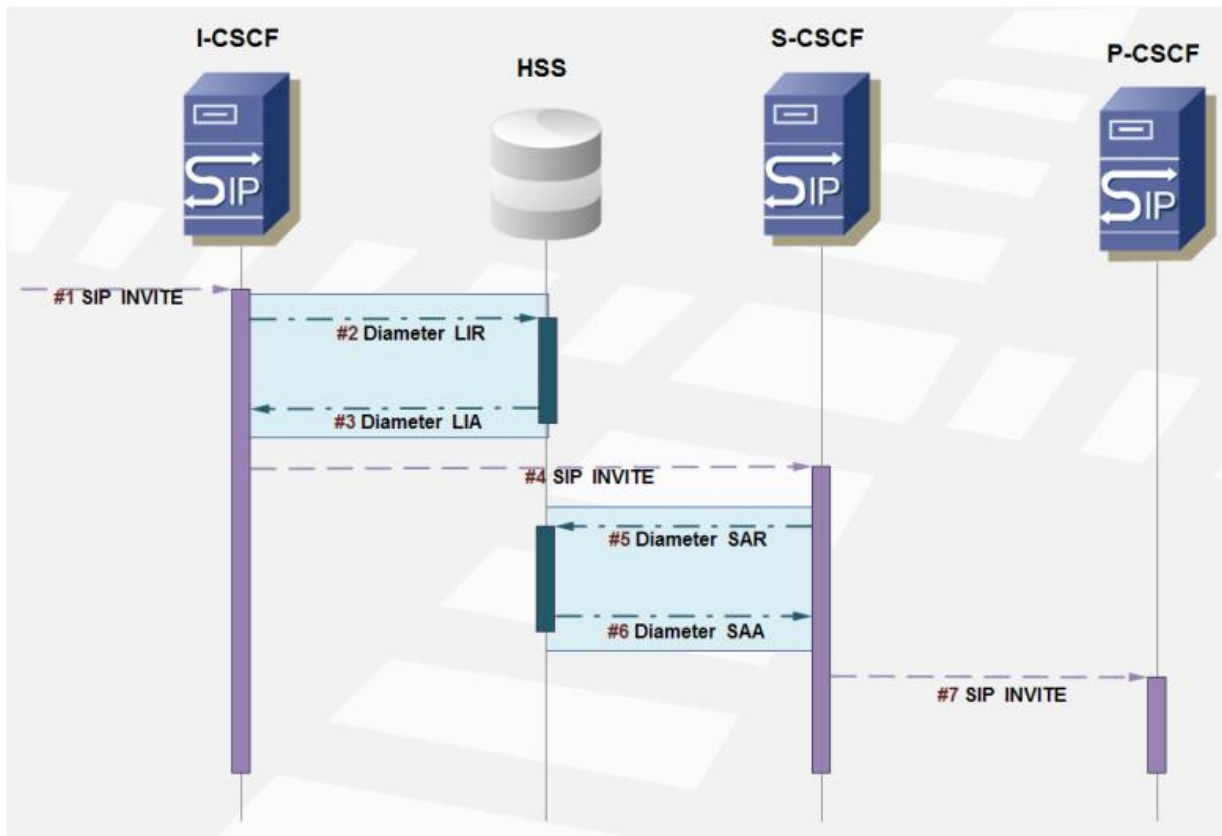


Figure F - 6. Use of Diameter LIR/LIA in the IMS SIP INVITE request with no «Route» header included.

### F.5.2 Policy and Charging Control (PCC) in the IMS

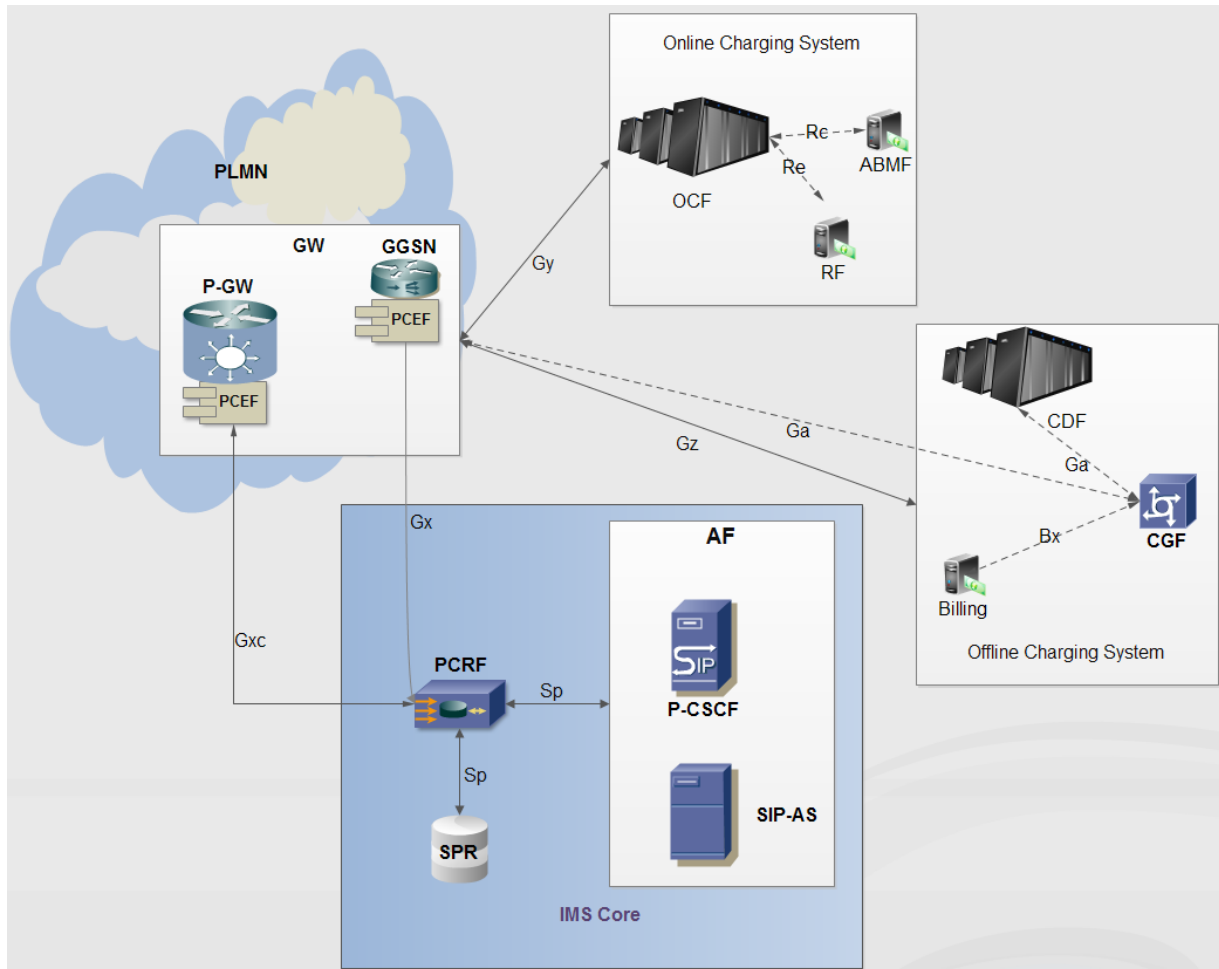


Figure F - 7. PCC Architecture in the IMS.

Next figure shows a call flow for control policy in «push mode», through which the PCRF conveys the policies to the Gateway, for a SIP INVITE incoming request.



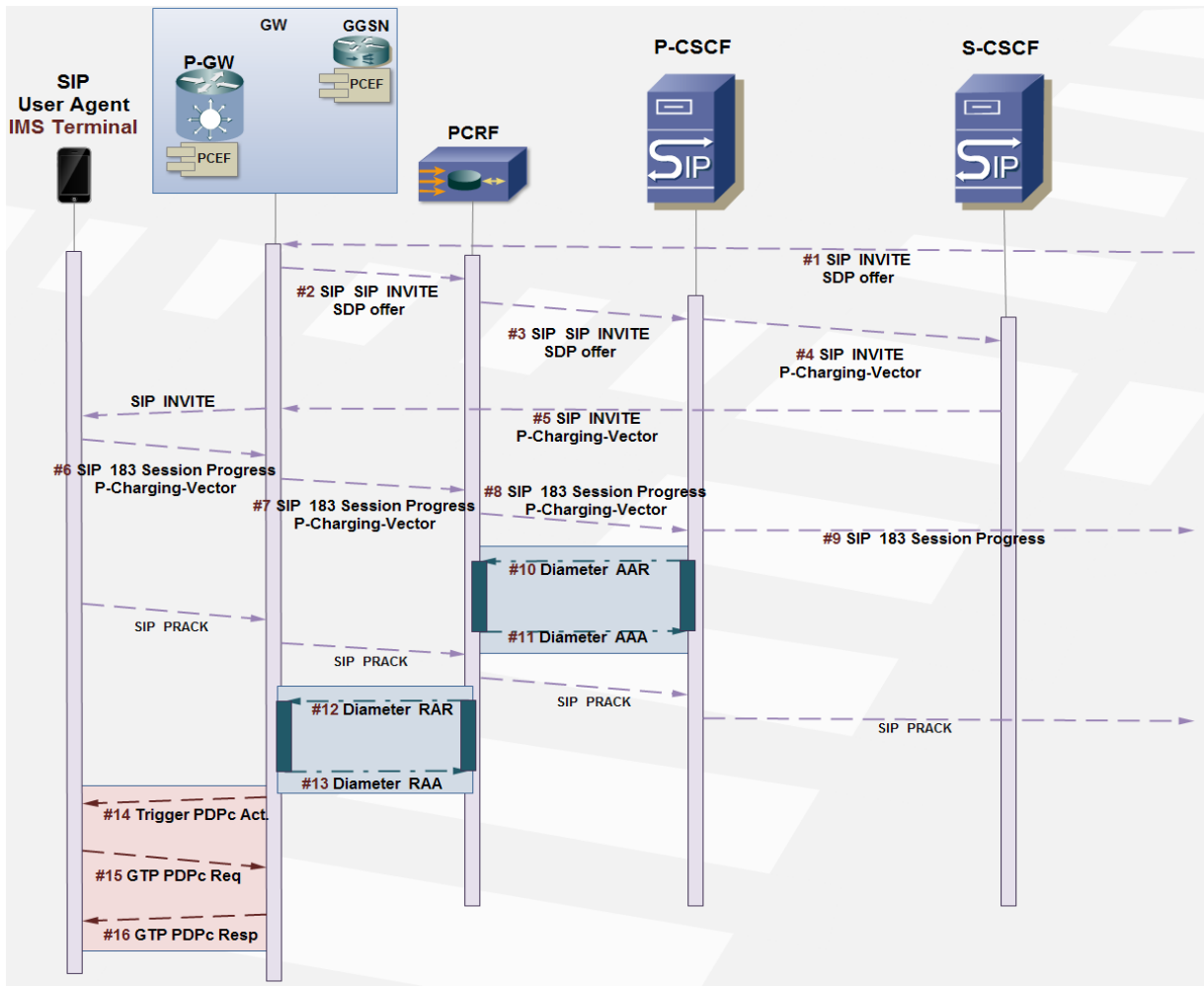


Figure F - 8. Push mode PCC call flow on incoming SIP INVITE request.

Next figure shows a call flow for control policy in «pull mode», through which the Gateway retrieves the policies to the PCRF, for a SIP INVITE incoming request.

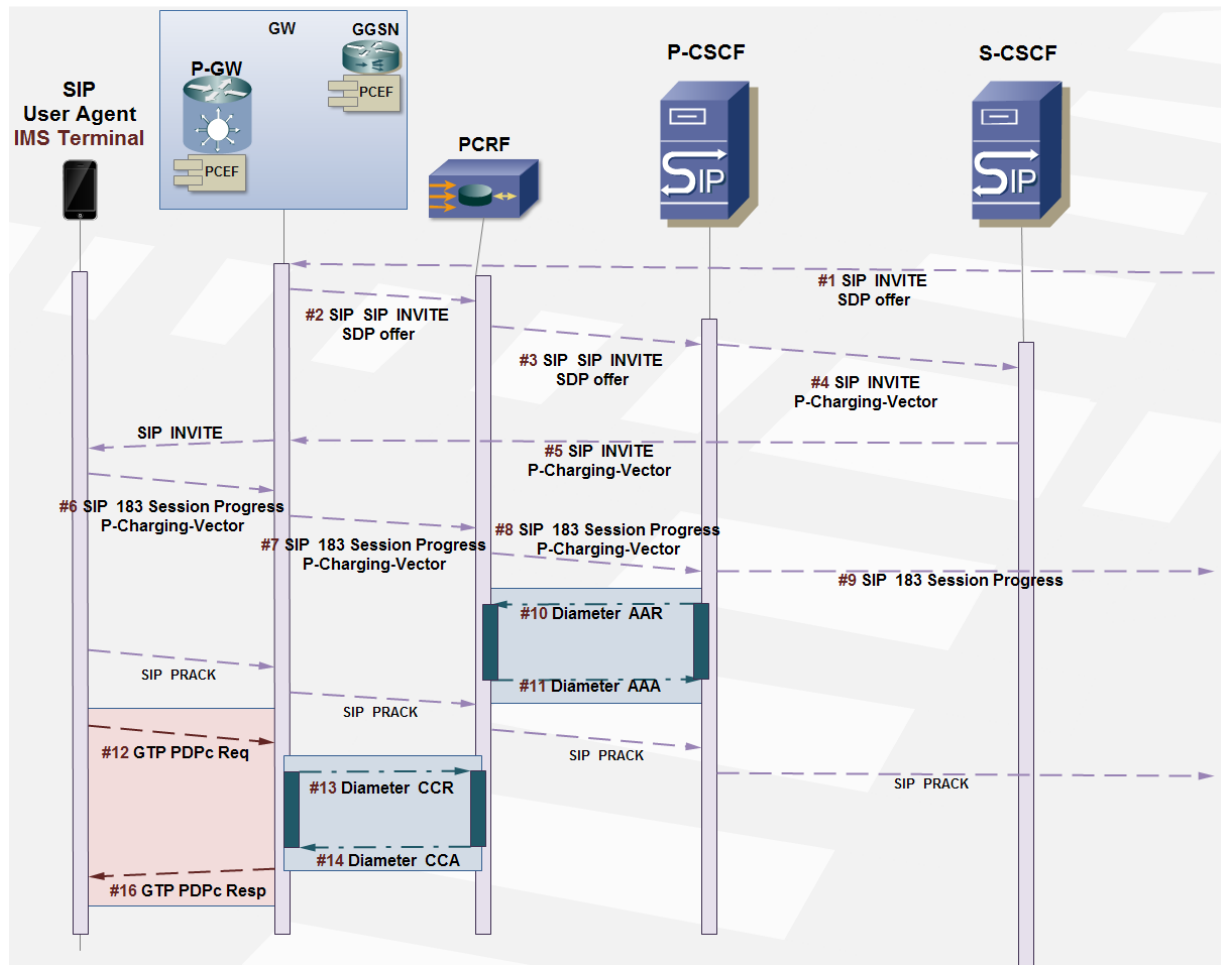


Figure F - 9. Pull mode PCC call flow on incoming SIP INVITE request.

Next figure shows a call flow for control policy in «push mode», through which the PCRF conveys the policies to the Gateway, for a SIP INVITE outgoing request.

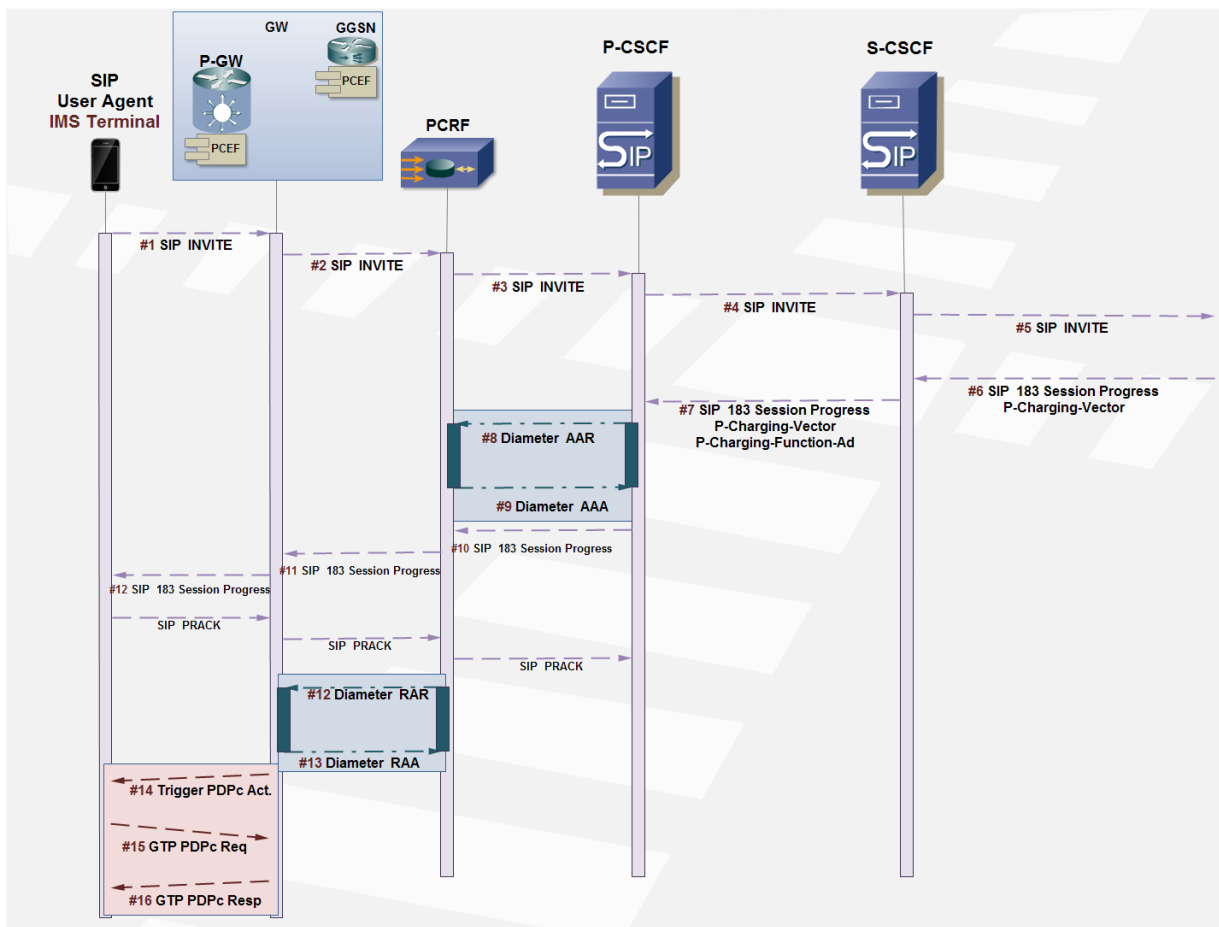


Figure F - 10. Push mode PCC call flow on outgoing SIP INVITE request.

Next figure shows a call flow for control policy in «pull mode», through which the Gateway retrieves the policies to the PCRF, for a SIP INVITE outgoing request.

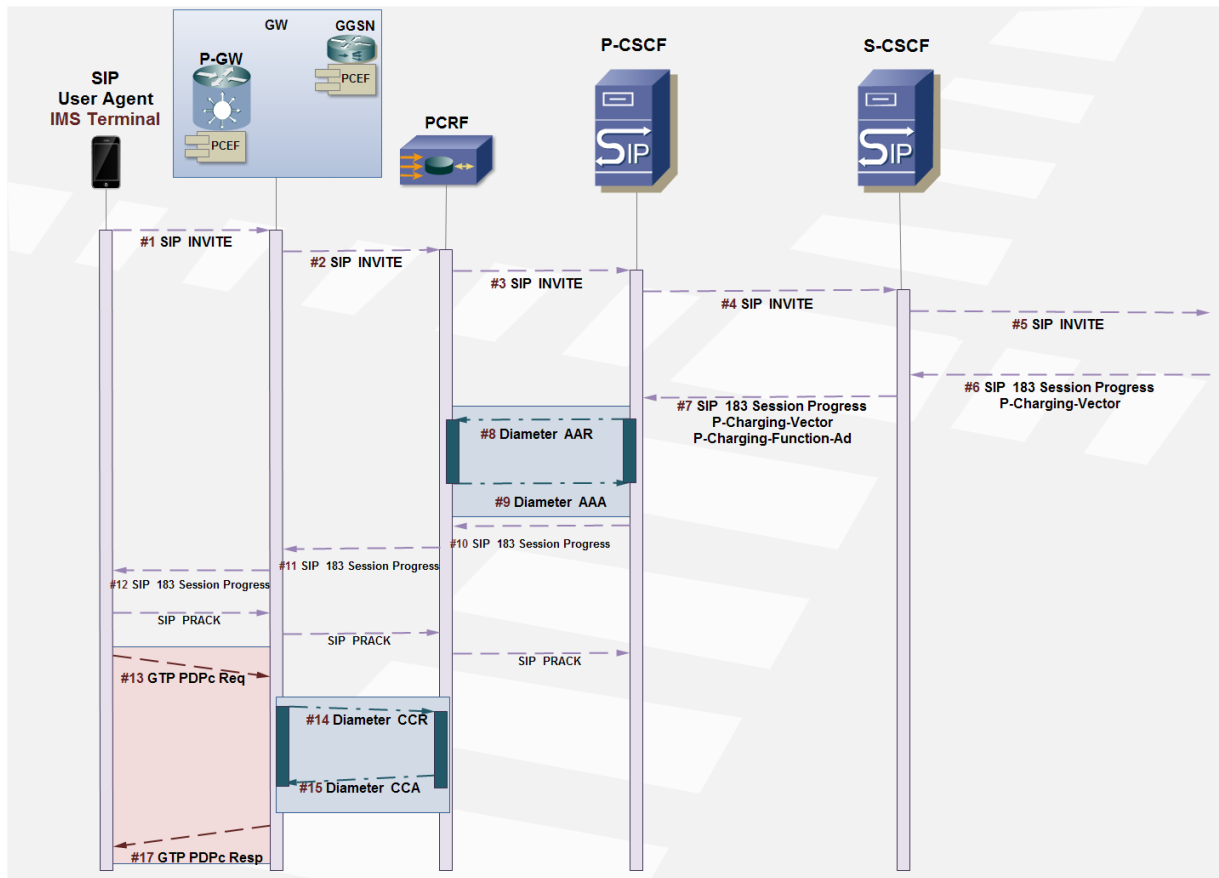


Figure F - 11. Pull mode PCC call flow on outgoing SIP INVITE request.

### F.5.2.1.1 PCC and Offline Charging Architecture in the IMS

Network elements introduced for charging record collections (Call Detail Records) in OFCS (Offline Charging System) for postpaid subscribers:

- CTF (Charging Trigger Function)
- CDF (Charging Data Function)

Offline charging architecture interfaces:

- Ga (GTP based): SBCF <-> ABMF
  - CDF<->CTF
  - CGF<->GGSN
  - CGF<->PDN-GW

- Rf (Diameter based)
  - CDF<->MRFC
  - CDF<->MGCF
  - CDF<->BGCF
  - CDF<->AS
  - CDF<->P-CSCF
  - CDF<->S-CSCF
  - CDF<->I-CSCF
- Bx: CGF<->Billing domain

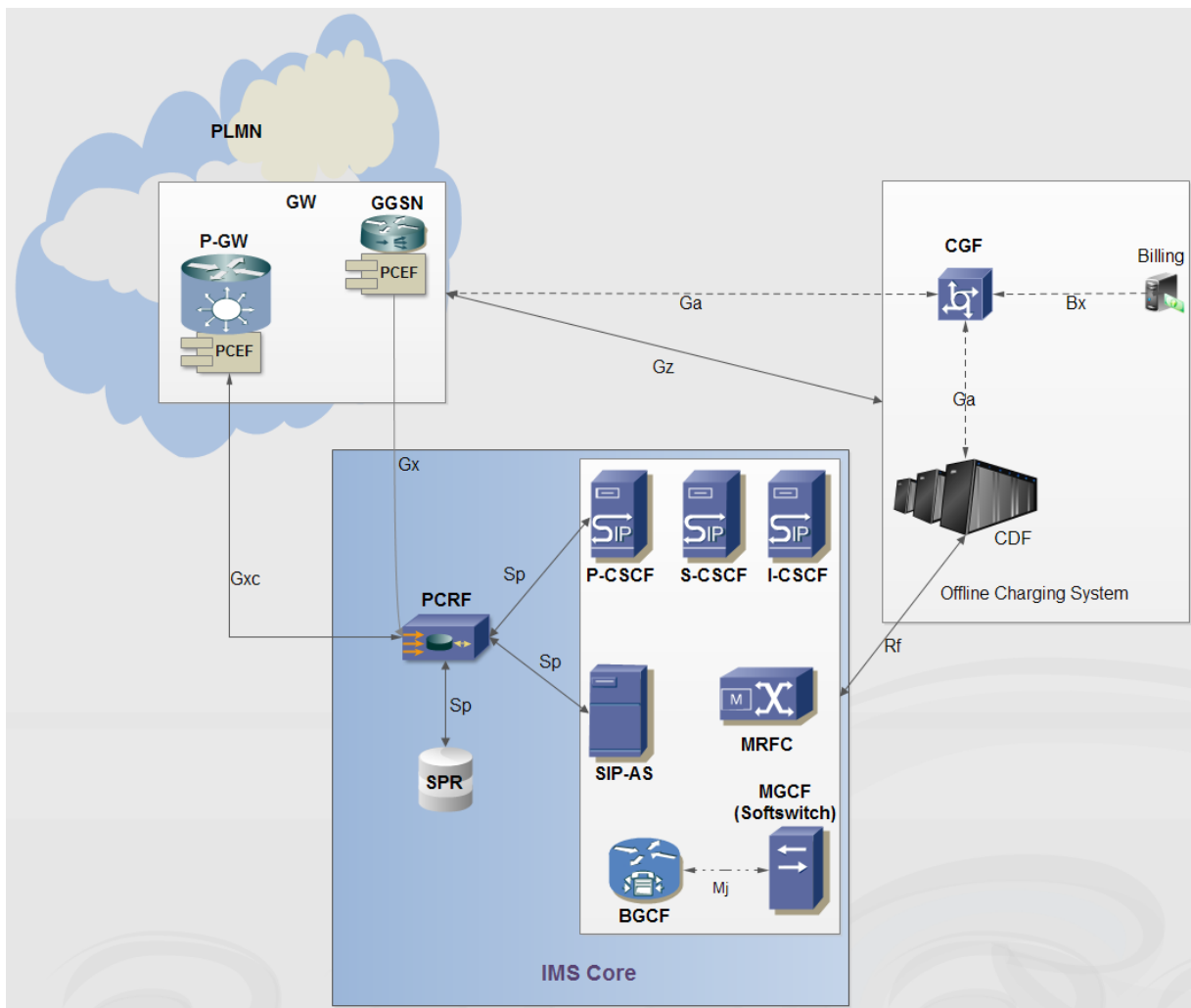


Figure F - 12. PCC in the IMS: Offline Charging Architecture.

Offline charging might be applied on events (e.g. after IM/SMS) or sessions.

**CTF** (Charging Trigger Function): Network elements enabled to collect charging metrics implement this charging processes triggering function. CTF generates charging events based on its accounting metrics, later sending these events to the CDF (Charging Data Function) over the Diameter based  $R_f$  interface. The CTF is deployed in network elements like P-CSCF, S-CSCF, I-CSCF, AS, MRFC, MGCF and the BGCF.

The CDF uses these accounting information events received over the  $R_f$  interface which are sent to the CGF (Charging Gateway Function) over GTP. The CGF acts as a gateway between the IMS and the billing domain, communication over the  $B_x$  interface, based on file transfer protocols (e.g. FTP) for CDR convey (as specified in 3GPP TS 32.297).

Next figure show a call flow for session establishment with offline charging as for PCC in the IMS.

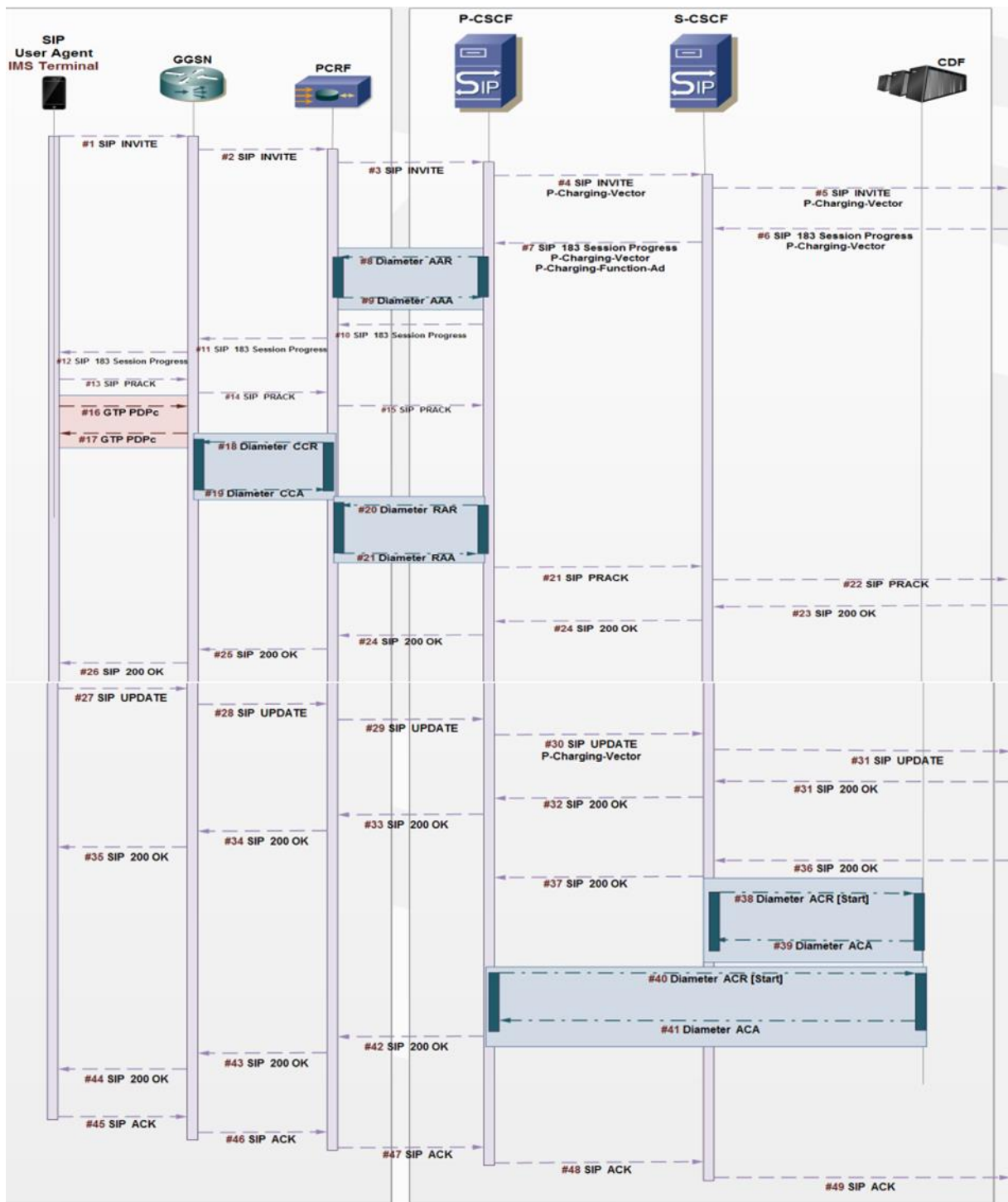


Figure F - 13. PCC in the IMS: session establishing call flow with Offline Charging.

### F.5.2.1.2 PCC and Online Charging Architecture in the IMS

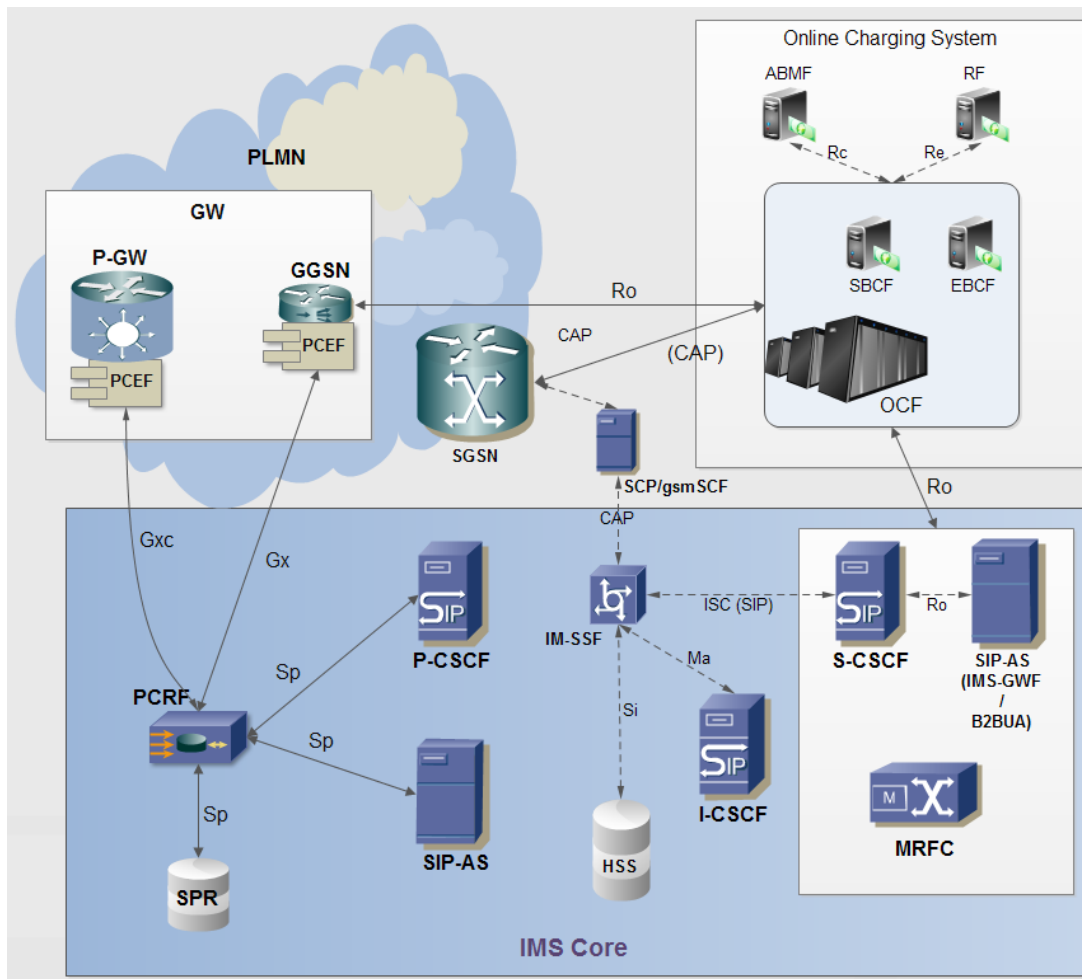


Figure F - 14. PCC in the IMS: Online Charging Architecture.

Network elements and functions introduced for online charging within OCS (Online Charging System) for prepaid subscribers:

- OCF (Online Charging Function):
  - SBCF (Session Based Charging Function)
  - EBCF (Event Based Charging Function)
- ABMF (Account Balance Management Function)
- RF (Rating Function)
- IMS GWF (IMS Gateway Function)
- CTF (Charging Triggering Function)



Online charging architecture interfaces:

- Rc: SBCF <-> ABMF
- Re: EBCF <-> RF
- Ro (Diameter based):
  - OCF <-> MRFC
  - OCF <-> GGSN
  - OCF <-> IMS-GW
  - OCF <-> AS
- IMS-GW <-> S-CSCF (ISC based)
- OCF <-> SGSN (CAP based)

Three types of online charging apply in the IMS:

➤ Immediate Event Charging (IEC):

- After an event, the OCF reserves an amount of credit units from the subscriber's account and then authorizes the CTF for providing service.

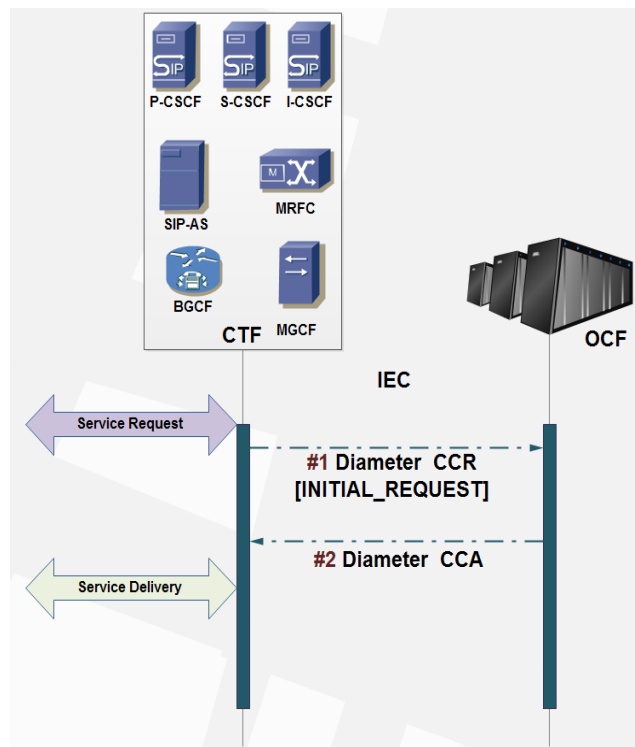


Figure F - 15. Immediate Event Charging (IEC) for Online Charging in the IMS.

- Event Charging with Unit Reservation (**ECUR**):
  - Event based charging.
  - The OCF reserves an amount of credit units from the subscriber's account and then authorizes the CTF for providing service.
  - If a particular service cost is greater than the amount of previously reserved credit units by the OCF, the CTF may contact an OCF for additional credit units' reservation.
  - When the service ends, the OCF makes the eventual refund of the credit units not used by the subscriber.

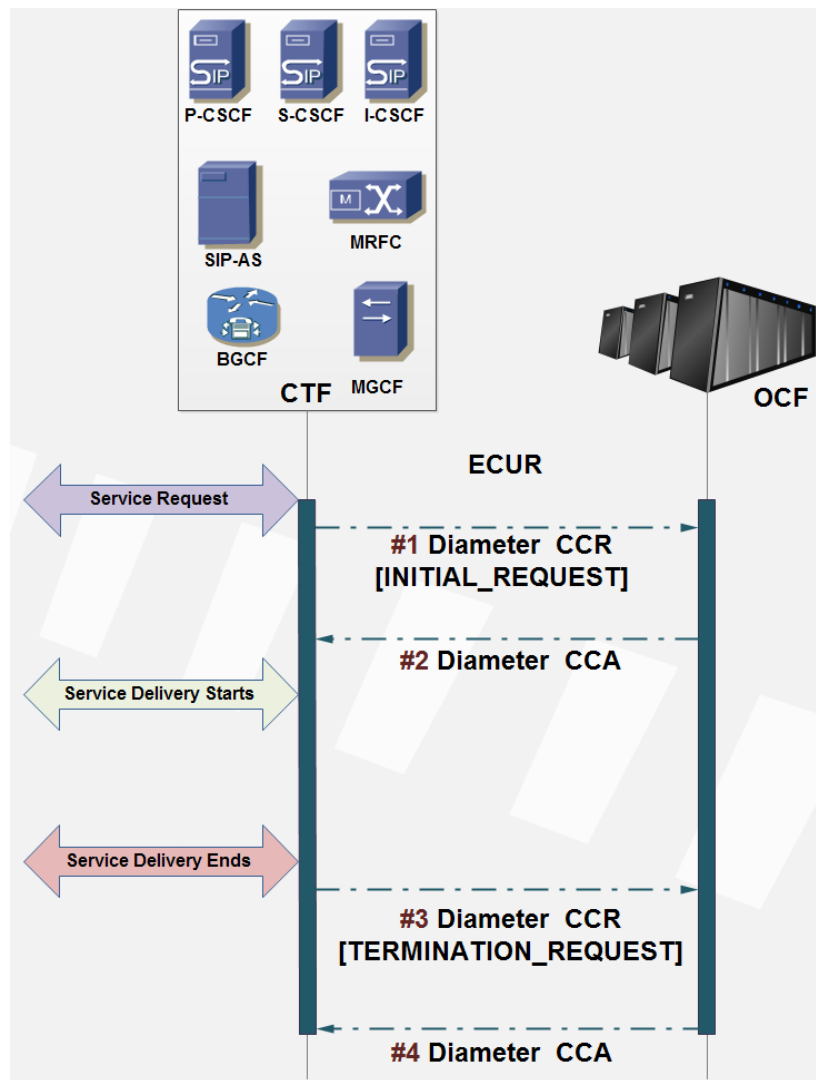


Figure F - 16. Event Charging with Unit Reservation (ECUR) for Online Charging in the IMS.

- Session Charging with Unit Reservation (**SCUR**):
  - Analogous to ECUR but for session charging, for which are used Diameter CCR/CCA with UPDATE REQUEST value for AVP CC-Request-Type.

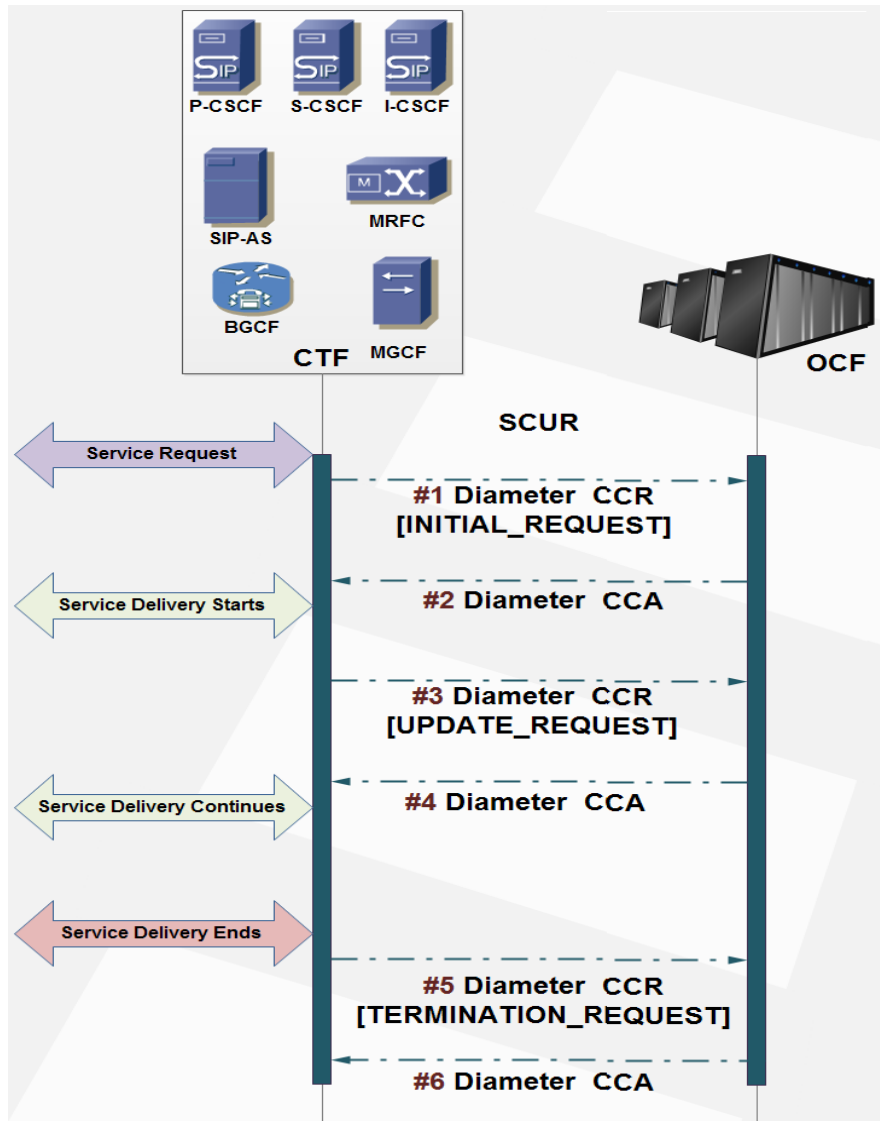


Figure F - 17. Session Charging with Unit Reservation (SCUR) for Online Charging in the IMS.

### F.5.3 Diameter AAA in VoLTE

Next figures show call flows for AAA in Voice over LTE via Diameter for offline charging.

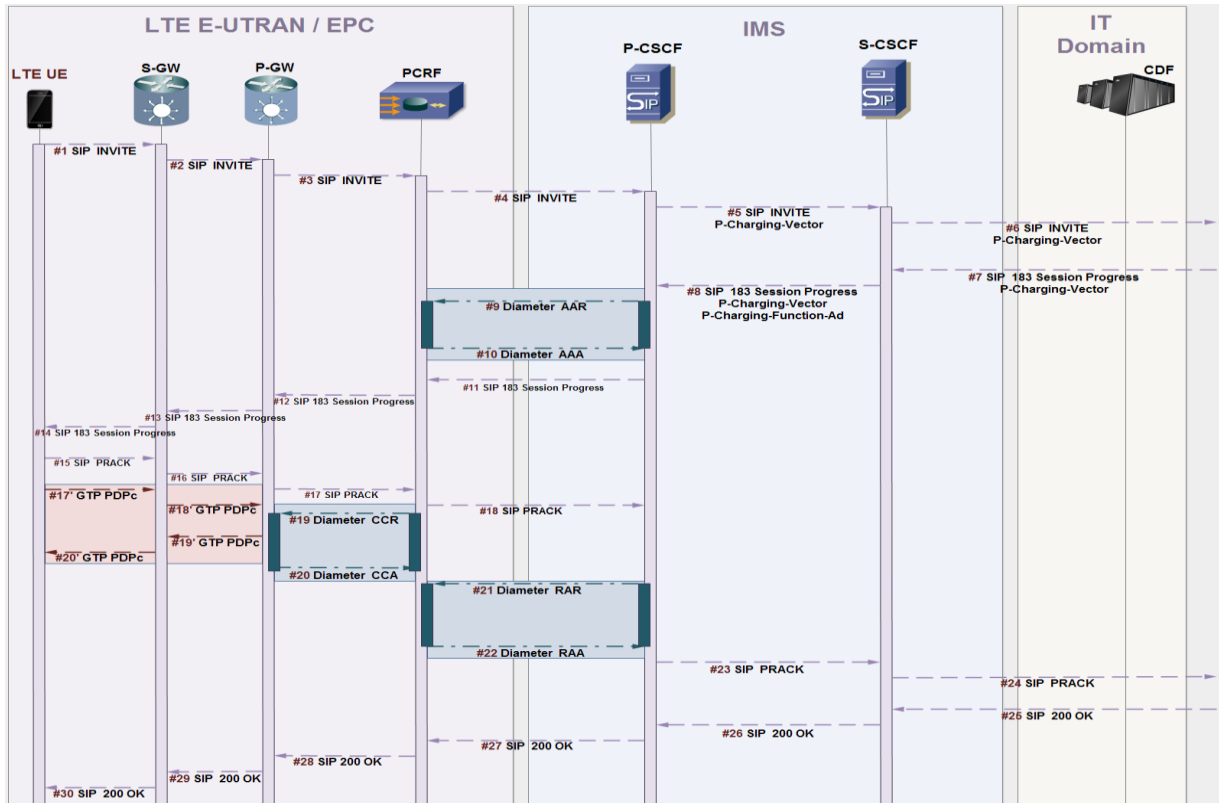


Figure F - 18. VoLTE call flow first stage: session establishment and AAA.

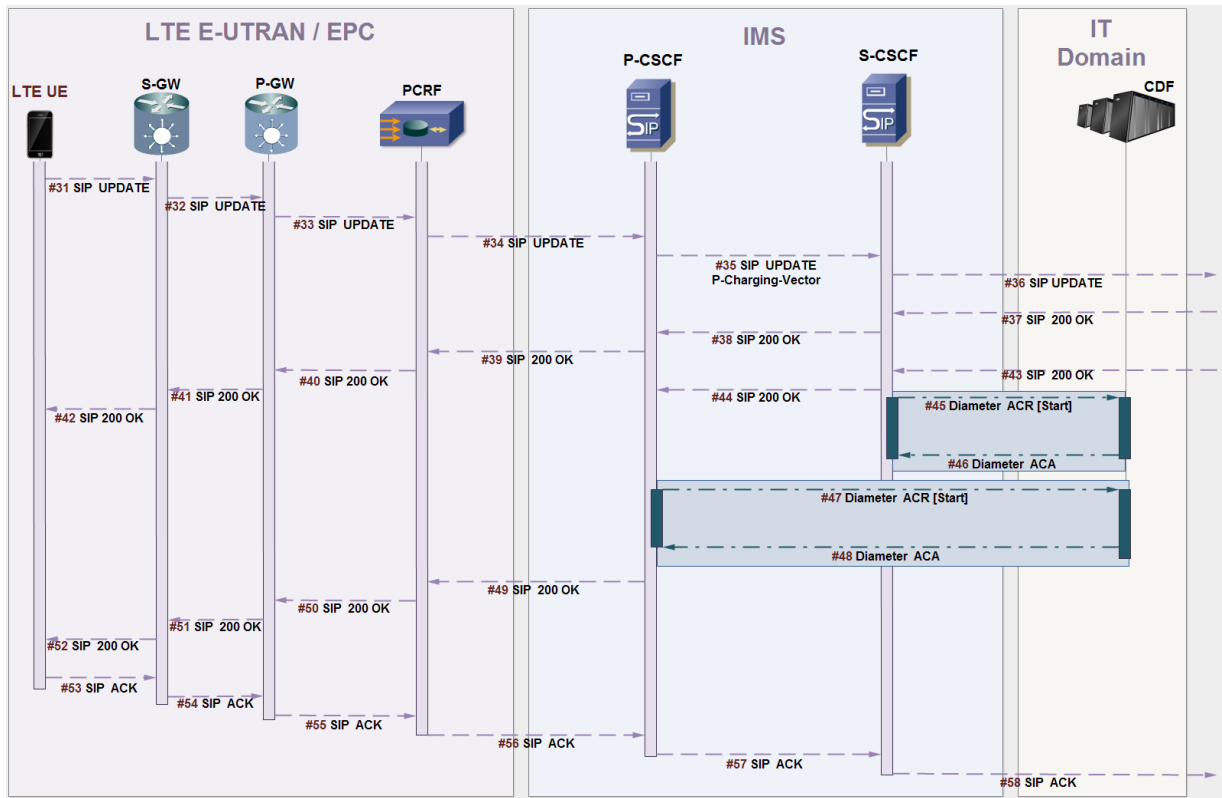


Figure F - 19. VoLTE call flow first stage: session update and online billing report.

## F.6 Introduction to RestComm jDiameter

RestComm jDiameter provides the only open source Diameter solution, spin off of the Mobicents project. It comprises following main characteristics:

- Diameter Stack supporting several Diameter interfaces/protocols like Diameter Base (IETF RFC 3588/6733), Credit-Control Application (IETF RFC 4006), Sh-Client/Server (3GPP TS 29.328/29.329), Ro/Rf (3GPP TS 32.260/32.299), Cx/Dx (3GPP TS 29.228/29.229), S13/S13' (3GPP TS 29.272) and now, SL<sub>h</sub> and SL<sub>g</sub> for LTE Location Services [44-45]. Diameter Stack is the core component of RestComm jDiameter solution. It is responsible for establishing and maintaining connections to other Diameter agents, routing of messages to other realms and peers and also control state of Diameter applications by implementing their state machines. It also provides means for validation of Diameter messages and AVPs (Attribute Value Pairs), capability of load balancing between peers and overload monitoring. Statistics are also provided by the stack.

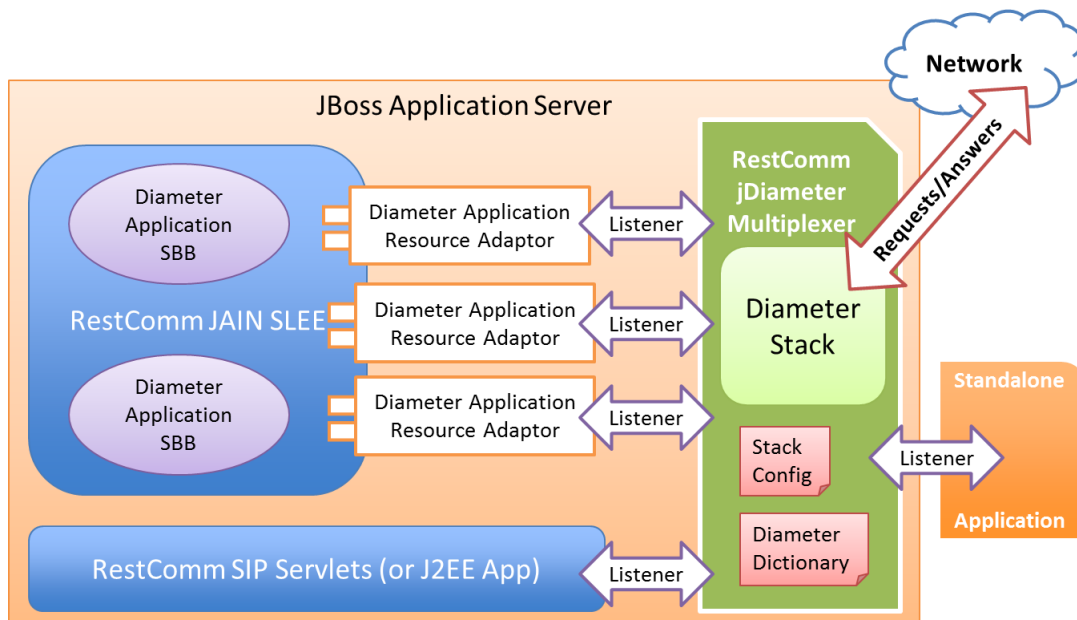


Figure F - 20. RestComm jDiameter basic architecture.

- Diameter session creation in the stack is performed when required and controlled by Session Factories, but the application is the only component holding reference to sessions. Diameter Sessions keep messages related to each other's in the same context and allow to receive and send messages. In Mobicents Diameter Stack they are defined by several interfaces, allowing extensions to be plugged at any layer and great reuse of existing resources. «RawSession» and «Session» life span is controlled entirely by the application, while the «<Application>Session» depends on the implemented state machine.

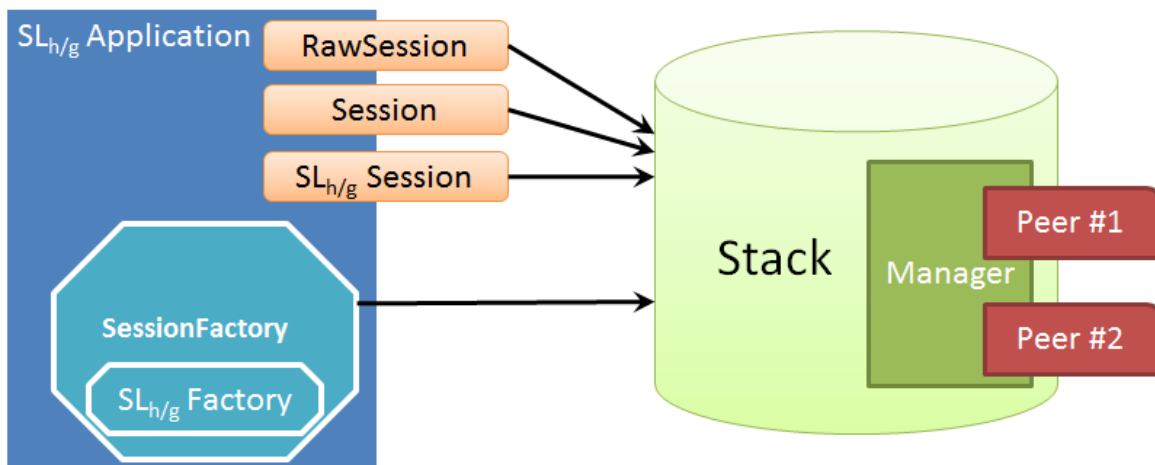


Figure F - 21. RestComm jDiameter Stack SL<sub>h/g</sub> application session control by corresponding Session Factory.

- RestComm jDiameter stack provides two useful functionalities for an easier and faster application development:
  - Dictionary: provides unified access to information regarding AVP structure, content and definition. Useful for retrieving AVP information by its name and/or code. All the information regarding an AVP (name, code, vendor-id, flags, etc.) can be retrieved with the dictionary. Dictionary is configured via an XML file named «dictionary.xml».
  - Validator: provides stack with the ability to validate messages. Useful for faster error detection, by validating both outgoing and incoming messages and AVPs. Validator uses the dictionary to verify the compliance.

- RestComm jDiameter Stack Multiplexer (MUX) provides the ability of sharing the stack between multiple applications. Entities interested in receiving messages for a certain Diameter application may register in the MUX. Upon registration, the entity passes the set of Application-Ids of its interest. Based on message content and registered listeners, MUX either drops message or passes it to a proper listener. MUX checks Application-Ids present in the message to match the target listener.

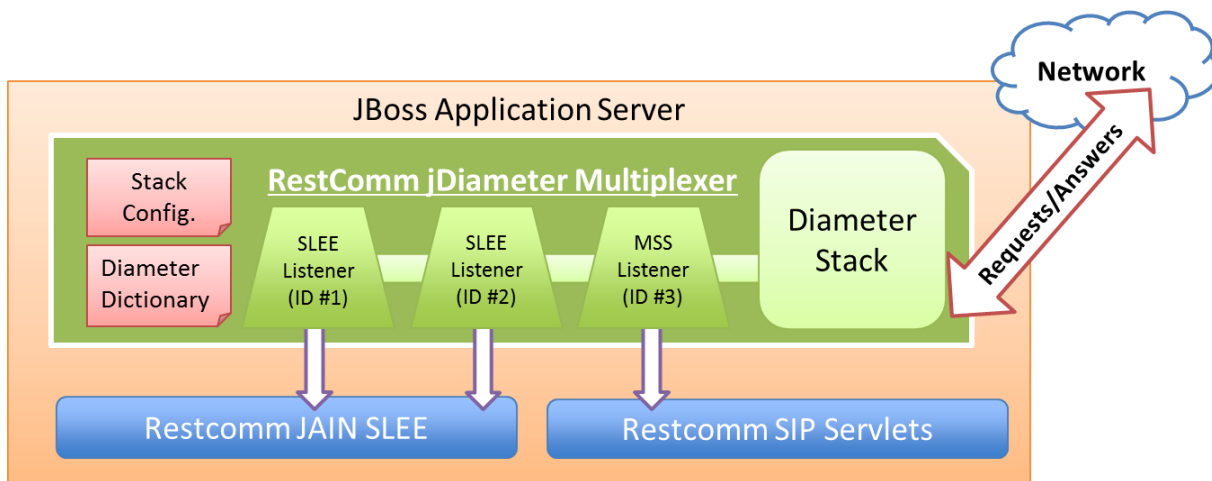


Figure F - 22. RestComm jDiameter MUX architecture.

- JAIN SLEE 1.0 and 1.1 [68] compatible Resource Adaptors for all of the above applications. JAIN SLEE (Java API for Integrated Networks Service Logic Execution Environment) specification [68] constitutes the JAVA community framework for the high standards in terms of performance, availability, portability, scalability, robustness, event oriented execution logic, etc., suitable for services/applications inter-working within telecommunication networks.

JAIN SLEE architecture, through its Resource Adaptors (RA), adjusts information from peripheral agents of the SLEE, namely: Mobile Switching Centre Servers (MSC/MSCS), Media Gateways (MGW, MGC/MGCF), Signaling Gateways (SGW), Mobility Management Entities (MME), SIP servers/proxies like Serving/Interrogating/Proxy-Call Session Control Functions



(S-CSCF, I-CSCF, P-CSCF), Media Resource Function Control, mobile subscribers data base query to HSS/HLR through Diameter/MAP respectively, Signaling Control Points (SCP) through CAP/INAP, and other service protocols like SOAP (Simple Object Access Protocol), OSA/Parlay, LDAP (Lightweight Directory Access Protocol), JDBC (Java Data Base Connectivity), JPA (Java Persistence API), etc. Beyond this work, Diameter queries for mobile subscribers under LTE by addressing the HSS and MME are also available by the introduction of such SLh and SLg RAs in RestComm JAIN SLEE Diameter implementation [134], along with RestComm jDiameter SLh and SLg interfaces development, already covered in previous sections of this annex (RestComm jDiameter Java archives are imported in RestComm JAIN SLEE Diameter RA implementations). As specified in [68, 135], the logic blocks exchanging information through this interfaces are called Resource Adaptors (RA), being their purpose the adaptation/abstraction of the complex information exchanged between the assorted external entities to a comprehensible format for the SLEE, specifically, Java objects (POJOs, EJBs) which represent events, so as to ease service development for consumption of underlying entities' capabilities.

The components that carry out logic implementation of services/applications according to JAIN SLEE are named Service Building Blocks or SBB. The SBB are executed within a «components container», which controls their life cycle and eases their composition. An SBB may comprise multiple child SBBs, which are also reusable for other services, encompassing Java code usually generated in a dynamic Service Creation Environment or SCE (e.g. RestComm Visual Designer RVD) or middleware platforms containing JAIN SLEE SBBs (e.g. RestComm GMLC).

JAIN SLEE service developer undergoes SBB construction by gathering logic items which represent events during the process of a service. As JAIN SLEE has been specially designed for event oriented logic execution, services are initiated by events like Diameter Requests/Answers. The generated SBBs then act together with the RAs under the JAIN SLEE framework so as to provide service to diverse external entities. Every arriving event at the SLEE through the RAs is distributed among the SBBs in order to process them. This

functionality is carried out by the «event router» as it is named within the functional structure of the JAIN SLEE framework. The next figure shows the basic logic architecture of the JAIN SLEE framework and jDiameter within a Restcomm Core Network Component and the external agents or peripheral network nodes.

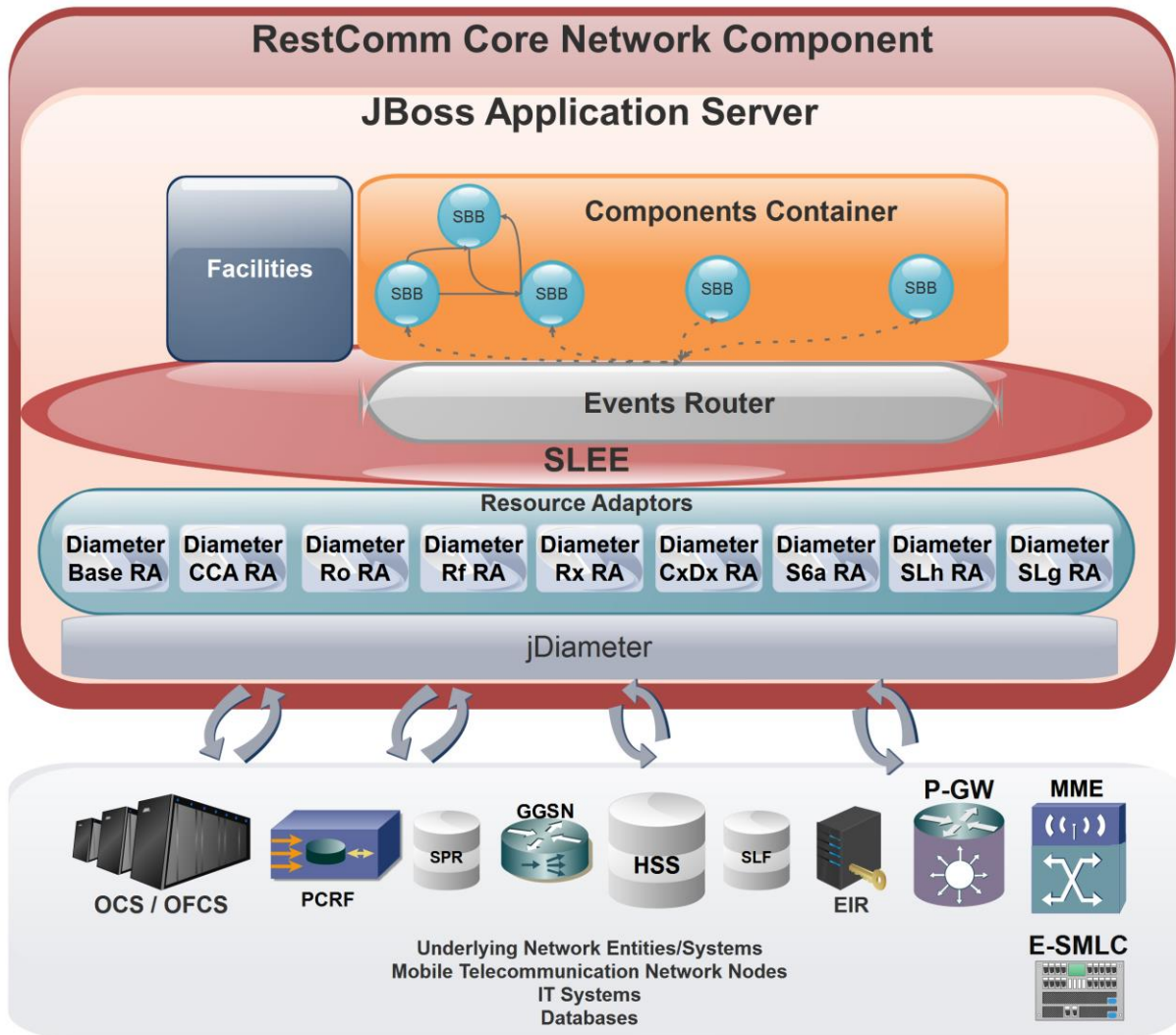


Figure F - 23. JAIN SLEE framework and jDiameter protocol stack within RestComm middleware core network entities' architecture and external agents or peripheral network nodes.

### F.6.1 SLh and SLg jDiameter implementation

Given the chosen framework for this work, implementation of SL<sub>g</sub> and SL<sub>h</sub> interfaces for LTE Location Services as defined in [44-45] were needed to be added to jDiameter. The work done for this implementation is public and can be reached at [130-132, 143-144]. All AVPs were implemented, and this section will provide examples of either interfaces commands execution, namely:

- Diameter Routing Information Request/Answer (RIR/RIA) over Diameter based SL<sub>h</sub> interface between GMLC and HSS: used to retrieve user equipment identities and core network entities routing information addresses to which send further location request over SL<sub>g</sub> interface between GMLC and MME.
- ELP Provide Location Request/Answer (PLR/PLA) over SL<sub>g</sub> interface between GMLC and MME: used to retrieve location information of a target User Equipment from the E-UTRAN (Evolved UMTS Terrestrial Radio Access Network), which should include location estimates in geographic coordinates of the target User Equipment, depending on available positioning methods (e.g. E-OTD, OTDOA, UTDOA, A-GPS, etc.).
- ELP Location Report Request/Answer (LRR/LRA) over SL<sub>g</sub> interface between MME and GMLC: used to gather location information of a target User Equipment from the E-UTRAN (or UTRAN/GERAN) when a request for location is either implicitly administered or made at some earlier time in ELP PLR/PLA for event based deferred type of location service.

#### F.6.1.1 SLh test example

This section portrays an example of RIR/RIA execution as the reader can trigger by using Junit testing after cloning RestComm jDiameter from source.

Only message's AVPs are shown for request/answer between Diameter client/server agents. These test examples include all possible AVPs defined by [45].

```

19:40:13,745 INFO [Client] Sending Request: 8388622 [E2E:198180868 -- HBH:1159945391 -- AppID:16777291]
19:40:13,745 INFO [Client] Request AVPs:
19:40:13,745 INFO [Client] <avp name="Session-Id" code="263" vendor="0" value="127.0.0.1;343;3307426062;xx-SLh-TESTxx" />
19:40:13,745 INFO [Client] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
19:40:13,746 INFO [Client] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
19:40:13,746 INFO [Client] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777291" />
19:40:13,746 INFO [Client] </avp>
19:40:13,746 INFO [Client] <avp name="Destination-Realm" code="283" vendor="0" value="server.mobicens.org" />
19:40:13,746 INFO [Client] <avp name="Origin-Realm" code="296" vendor="0" value="client.mobicens.org" />
19:40:13,746 INFO [Client] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
19:40:13,746 INFO [Client] <avp name="Origin-Host" code="264" vendor="0" value="aaa://127.0.0.1:13868" />
19:40:13,746 INFO [Client] <avp name="3GPP-IMSI" code="1" vendor="10415" value="748039876543210" />
19:40:13,746 INFO [Client] <avp name="MSISDN" code="701" vendor="10415" value="59899077937" />
19:40:13,746 INFO [Client] <avp name="GMLC-Number" code="1474" vendor="10415" value="759834279" />

```

Figure F - 24. jDiameter SL<sub>h</sub> RIR example (sample containing all AVPs executed).

```

19:40:15,786 INFO [Server] Sending Answer: 8388622 [E2E:198180868 -- HBH:1159945391 -- AppID:16777291]
19:40:15,786 INFO [Server] Request AVPs:
19:40:15,786 INFO [Server] <avp name="Session-Id" code="263" vendor="0" value="127.0.0.1;343;3307426062;xx-SLh-TESTxx" />
19:40:15,786 INFO [Server] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
19:40:15,786 INFO [Server] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
19:40:15,786 INFO [Server] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777291" />
19:40:15,786 INFO [Server] </avp>
19:40:15,786 INFO [Server] <avp name="Result-Code" code="268" vendor="0" value="2001" />
19:40:15,786 INFO [Server] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
19:40:15,786 INFO [Server] <avp name="3GPP-IMSI" code="1" vendor="10415" value="748039876543210" />
19:40:15,786 INFO [Server] <avp name="MSISDN" code="701" vendor="10415" value="59899077937" />
19:40:15,786 INFO [Server] <avp name="IMSI" code="2400" vendor="10415" value="748031234567890" />
19:40:15,786 INFO [Server] <avp name="Serving-Node" code="2401" vendor="10415">
19:40:15,786 INFO [Server] <avp name="SGSN-Number" code="1489" vendor="10415" value="59899004501" />
19:40:15,786 INFO [Server] <avp name="SGSN-Name" code="2409" vendor="10415" value="SGSN01" />
19:40:15,786 INFO [Server] <avp name="SGSN-Realm" code="2410" vendor="10415" value="sgsn.restcomm.com" />
19:40:15,786 INFO [Server] <avp name="MME-Name" code="2402" vendor="10415" value="MME710" />
19:40:15,786 INFO [Server] <avp name="MME-Realm" code="2408" vendor="10415" value="mme.restcomm.com" />
19:40:15,786 INFO [Server] <avp name="MSC-Number" code="2403" vendor="10415" value="59899001207" />
19:40:15,786 INFO [Server] <avp name="3GPP-AAA-Server-Name" code="318" vendor="10415" value="aaa.restcomm.com" />
19:40:15,786 INFO [Server] <avp name="LCS-Capabilities-Sets" code="2404" vendor="10415" value="99900123" />
19:40:15,786 INFO [Server] <avp name="GMLC-Address" code="2405" vendor="10415" value="2001:0:9d38:6abd:ca4:721:58c6:a159" />
19:40:15,786 INFO [Server] </avp>
19:40:15,786 INFO [Server] <avp name="Additional-Serving-Node" code="2406" vendor="10415">
19:40:15,786 INFO [Server] <avp name="SGSN-Number" code="1489" vendor="10415" value="59899004502" />
19:40:15,786 INFO [Server] <avp name="SGSN-Name" code="2409" vendor="10415" value="SGSN02" />
19:40:15,787 INFO [Server] <avp name="SGSN-Realm" code="2410" vendor="10415" value="sgsn2.restcomm.com" />
19:40:15,787 INFO [Server] <avp name="MME-Name" code="2402" vendor="10415" value="MME712" />
19:40:15,787 INFO [Server] <avp name="MME-Realm" code="2408" vendor="10415" value="mme2.restcomm.com" />
19:40:15,787 INFO [Server] <avp name="MSC-Number" code="2403" vendor="10415" value="59899001210" />
19:40:15,787 INFO [Server] <avp name="3GPP-AAA-Server-Name" code="318" vendor="10415" value="aaa2.restcomm.com" />
19:40:15,787 INFO [Server] <avp name="LCS-Capabilities-Sets" code="2404" vendor="10415" value="88800123" />
19:40:15,787 INFO [Server] <avp name="GMLC-Address" code="2405" vendor="10415" value="2001:0:9d38:6abd:ca4:721:58c6:a158" />
19:40:15,787 INFO [Server] </avp>
19:40:15,787 INFO [Server] <avp name="PPR-Address" code="2407" vendor="10415" value="2001:0:9d38::ca4:721:58c6:a159" />
19:40:15,787 INFO [Server] <avp name="RIA-Flags" code="2411" vendor="10415" value="0" />
19:40:15,787 INFO [Server] <avp name="Origin-Host" code="264" vendor="0" value="127.0.0.1" />
19:40:15,787 INFO [Server] <avp name="Origin-Realm" code="296" vendor="0" value="server.mobicens.org" />
19:40:15,787 INFO [Server]

```

Figure F - 25. jDiameter SL<sub>h</sub> RIA example (sample containing all AVPs executed).

### F.6.1.2 SL<sub>g</sub> test example

This section portrays an example of PLR/PLA execution as the reader can trigger by using Junit testing after cloning RestComm jDiameter from source. Only message's AVPs are shown for request/answer between Diameter client/server agents.

These examples include all possible AVPs as defined by [44] for PLR/PLA and LRR/LRA.

```

19:16:02,503 INFO [ClientPLR] Sending Request: 8388620 [E2E:2032140292 -- HBH:1417694393 -- AppID:16777255]
19:16:02,503 INFO [ClientPLR] Request AVPs:
19:16:02,503 INFO [ClientPLR] <avp name="Session-Id" code="263" vendor="0" value="127.0.0.1;343;3565175303;xx-SLg-TESTxx" />
19:16:02,503 INFO [ClientPLR] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
19:16:02,503 INFO [ClientPLR] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
19:16:02,503 INFO [ClientPLR] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
19:16:02,503 INFO [ClientPLR] </avp>
19:16:02,503 INFO [ClientPLR] <avp name="Destination-Realm" code="283" vendor="0" value="server.mobicients.org" />
19:16:02,503 INFO [ClientPLR] <avp name="Origin-Realm" code="296" vendor="0" value="client.mobicients.org" />
19:16:02,503 INFO [ClientPLR] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
19:16:02,503 INFO [ClientPLR] <avp name="Origin-Host" code="264" vendor="0" value="aaa://127.0.0.1:13868" />
19:16:02,503 INFO [ClientPLR] <avp name="SLg-Location-Type" code="2500" vendor="10415" value="0" />
19:16:02,504 INFO [ClientPLR] <avp name="3GPP-IMSI" code="1" vendor="10415" value="748039876543210" />
19:16:02,504 INFO [ClientPLR] <avp name="MSISDN" code="701" vendor="10415" value="59899077937" />
19:16:02,504 INFO [ClientPLR] <avp name="IMEI" code="1402" vendor="10415" value="011714004661057" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-EPS-Client-Name" code="2501" vendor="10415">
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Name-String" code="1238" vendor="10415" value="Restcomm Geolocation API" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Format-Indicator" code="1237" vendor="10415" value="2" />
19:16:02,504 INFO [ClientPLR] </avp>
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Client-Type" code="1241" vendor="10415" value="1" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Requestor-Name" code="2502" vendor="10415">
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Requestor-Id-String" code="1240" vendor="10415" value="restcomm_geolocation_23" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Format-Indicator" code="1237" vendor="10415" value="3" />
19:16:02,504 INFO [ClientPLR] </avp>
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Priority" code="2503" vendor="10415" value="0" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-QoS" code="2504" vendor="10415">
19:16:02,504 INFO [ClientPLR] <avp name="LCS-QoS-Class" code="2523" vendor="10415" value="1" />
19:16:02,504 INFO [ClientPLR] <avp name="Horizontal-Accuracy" code="2505" vendor="10415" value="120" />
19:16:02,504 INFO [ClientPLR] <avp name="Vertical-Accuracy" code="2506" vendor="10415" value="3237" />
19:16:02,504 INFO [ClientPLR] <avp name="Vertical-Requested" code="2507" vendor="10415" value="0" />
19:16:02,504 INFO [ClientPLR] <avp name="Response-Time" code="2509" vendor="10415" value="1" />
19:16:02,504 INFO [ClientPLR] </avp>
19:16:02,504 INFO [ClientPLR] <avp name="Velocity-Requested" code="2508" vendor="10415" value="0" />
19:16:02,504 INFO [ClientPLR] <avp name="Supported-GAD-Shapes" code="2510" vendor="10415" value="3" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Service-Type-ID" code="2520" vendor="10415" value="234" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Codeword" code="2511" vendor="10415" value="rgl49f9f$#ERSD" />
19:16:02,504 INFO [ClientPLR] <avp name="Service-Selection" code="493" vendor="0" value="restcomm.org" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Privacy-Check-Session" code="2522" vendor="10415">
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Privacy-Check" code="2512" vendor="10415" value="2" />
19:16:02,504 INFO [ClientPLR] </avp>
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Privacy-Check-Session" code="2522" vendor="10415">
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Privacy-Check" code="2512" vendor="10415" value="2" />
19:16:02,504 INFO [ClientPLR] </avp>
19:16:02,504 INFO [ClientPLR] <avp name="Deferred-Location-Type" code="2532" vendor="10415" value="8" />
19:16:02,504 INFO [ClientPLR] <avp name="LCS-Reference-Number" code="2531" vendor="10415" value="579" />
19:16:02,504 INFO [ClientPLR] <avp name="Area-Event-Info" code="2533" vendor="10415">
19:16:02,504 INFO [ClientPLR] <avp name="Occurrence-Info" code="2538" vendor="10415" value="1" />
19:16:02,504 INFO [ClientPLR] </avp>
19:16:02,504 INFO [ClientPLR] <avp name="Area-Definition" code="2534" vendor="10415">
19:16:02,504 INFO [ClientPLR] <avp name="Area-Type" code="2536" vendor="10415" value="3" />
19:16:02,504 INFO [ClientPLR] <avp name="Area-Identification" code="2537" vendor="10415" value="area51" />
19:16:02,504 INFO [ClientPLR] </avp>
19:16:02,505 INFO [ClientPLR] <avp name="GMLC-Address" code="2405" vendor="10415" value="2001:0:5ef5:79fb:3403:11a4:58c7:f7da" />
19:16:02,505 INFO [ClientPLR] <avp name="PLR-Flags" code="2545" vendor="10415" value="4" />
19:16:02,505 INFO [ClientPLR] <avp name="Area-Event-Info" code="2533" vendor="10415">
19:16:02,505 INFO [ClientPLR] <avp name="Reporting-Amount" code="2541" vendor="10415" value="8639910" />
19:16:02,505 INFO [ClientPLR] <avp name="Reporting-Interval" code="2542" vendor="10415" value="8639998" />
19:16:02,505 INFO [ClientPLR] </avp>
19:16:02,505 INFO [ClientPLR] <avp name="Reporting-PLMN-List" code="2543" vendor="10415">
19:16:02,505 INFO [ClientPLR] <avp name="Prioritized-List-Indicator" code="2551" vendor="10415" value="0" />
19:16:02,505 INFO [ClientPLR] <avp name="PLMN-ID-List" code="2544" vendor="10415">
19:16:02,505 INFO [ClientPLR] </avp>
19:16:02,505 INFO [ClientPLR] </avp>
19:16:02,505 INFO [ClientPLR] <avp name="PLMN-ID-List" code="2544" vendor="10415">
19:16:02,505 INFO [ClientPLR] <avp name="Visited-PLMN-Id" code="1407" vendor="10415" value="74803, 74801" />
19:16:02,505 INFO [ClientPLR] <avp name="Periodic-Location-Support-Indicator" code="2550" vendor="10415" value="1" />
19:16:02,505 INFO [ClientPLR] </avp>

```

Figure F - 26. jDiameter SLg PLR example (sample containing all AVPs executed).



```

19:16:04,533 INFO [ServerPLA] Sending Answer: 8388620 [EZE:2032140292 -- HBH:1417694393 -- AppID:16777255]
19:16:04,533 INFO [ServerPLA] Request AVPs:
19:16:04,533 INFO [ServerPLA] <avp name="Session-Id" code="263" vendor="0" value="127.0.0.1;343;3565175303;xx-SLg-TESTxx" />
19:16:04,533 INFO [ServerPLA] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0">
19:16:04,533 INFO [ServerPLA] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
19:16:04,533 INFO [ServerPLA] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
19:16:04,533 INFO [ServerPLA] </avp>
19:16:04,533 INFO [ServerPLA] <avp name="Result-Code" code="268" vendor="0" value="2001" />
19:16:04,533 INFO [ServerPLA] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
19:16:04,533 INFO [ServerPLA] <avp name="Location-Estimate" code="1242" vendor="10415" value="S35°38'15.37" WE109°45'21.77"" />
19:16:04,533 INFO [ServerPLA] <avp name="Accuracy-Fulfilment-Indicator" code="2513" vendor="10415" value="0" />
19:16:04,533 INFO [ServerPLA] <avp name="Age-Of-Location-Estimate" code="2514" vendor="10415" value="0" />
19:16:04,533 INFO [ServerPLA] <avp name="Velocity-Estimate" code="2515" vendor="10415" value="200mph" />
19:16:04,533 INFO [ServerPLA] <avp name="EUTRAN-Positioning-Data" code="2516" vendor="10415" value="eNB4531tea23" />
19:16:04,533 INFO [ServerPLA] <avp name="ECGI" code="2517" vendor="10415" value="eNB9437" />
19:16:04,533 INFO [ServerPLA] <avp name="GERAN-Positioning-Info" code="2524" vendor="10415">
19:16:04,533 INFO [ServerPLA] <avp name="GERAN-Positioning-Data" code="2525" vendor="10415" value="BTS943BSC3" />
19:16:04,533 INFO [ServerPLA] <avp name="GERAN-GANSS-Positioning-Data" code="2526" vendor="10415" value="BTS73RNC1Ganss43" />
19:16:04,533 INFO [ServerPLA] </avp>
19:16:04,533 INFO [ServerPLA] <avp name="Cell-Global-Identity" code="1604" vendor="10415" value="9342784713907" />
19:16:04,533 INFO [ServerPLA] <avp name="UTRAN-Positioning-Info" code="2527" vendor="10415">
19:16:04,533 INFO [ServerPLA] <avp name="UTRAN-Positioning-Data" code="2528" vendor="10415" value="NB943RNC1" />
19:16:04,533 INFO [ServerPLA] <avp name="UTRAN-GANSS-Positioning-Data" code="2529" vendor="10415" value="NB031RNC5Ganss43" />
19:16:04,533 INFO [ServerPLA] </avp>
19:16:04,533 INFO [ServerPLA] <avp name="Service-Area-Identity" code="1607" vendor="10415" value="service-area-umts-3" />
19:16:04,533 INFO [ServerPLA] <avp name="Serving-Node" code="2401" vendor="10415">
19:16:04,533 INFO [ServerPLA] <avp name="SGSN-Number" code="1489" vendor="10415" value="59899004501" />
19:16:04,533 INFO [ServerPLA] <avp name="SGSN-Name" code="2409" vendor="10415" value="SGSN01" />
19:16:04,533 INFO [ServerPLA] <avp name="SGSN-Realm" code="2410" vendor="10415" value="sgsn.restcomm.com" />
19:16:04,533 INFO [ServerPLA] <avp name="MME-Name" code="2402" vendor="10415" value="MME710" />
19:16:04,533 INFO [ServerPLA] <avp name="MME-Realm" code="2408" vendor="10415" value="mme.restcomm.com" />
19:16:04,533 INFO [ServerPLA] <avp name="MSC-Number" code="2403" vendor="10415" value="59899001207" />
19:16:04,533 INFO [ServerPLA] <avp name="3GPP-AAA-Server-Name" code="318" vendor="10415" value="aaa.restcomm.com" />
19:16:04,533 INFO [ServerPLA] <avp name="LCS-Capabilities-Sets" code="2404" vendor="10415" value="99900123" />
19:16:04,533 INFO [ServerPLA] <avp name="GMLC-Address" code="2405" vendor="10415" value="2001:0:5ef5:79fb:3403:11a4:58c7:f7da" />
19:16:04,533 INFO [ServerPLA] </avp>
19:16:04,533 INFO [ServerPLA] <avp name="PLA-Flags" code="2546" vendor="10415" value="0" />
19:16:04,533 INFO [ServerPLA] <avp name="ESMLC-Cell-Info" code="2552" vendor="10415">
19:16:04,533 INFO [ServerPLA] <avp name="ECGI" code="2517" vendor="10415" value="eNB9437" />
19:16:04,533 INFO [ServerPLA] <avp name="Cell-Portion-ID" code="2553" vendor="10415" value="0" />
19:16:04,533 INFO [ServerPLA] </avp>
19:16:04,533 INFO [ServerPLA] <avp name="Civic-Address" code="2556" vendor="10415" value="<civicAddress xml:lang="en-US"
  xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
  xmlns:cae="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr:ext">
  <country>US</country>
  <A1>CA</A1>
  <A2>Sacramento</A2>
  <RD>Colorado</RD>
  <HNO>223</HNO>
  <cae:STP>Boulevard</cae:STP>
  <cae:HNP>A</cae:HNP>
</civicAddress>" />
19:16:04,533 INFO [ServerPLA] <avp name="Barometric-Pressure" code="2557" vendor="10415" value="101327" />
19:16:04,533 INFO [ServerPLA] <avp name="Origin-Host" code="264" vendor="0" value="127.0.0.1" />
19:16:04,533 INFO [ServerPLA] <avp name="Origin-Realm" code="296" vendor="0" value="server.mobicients.org" />

```

Figure F - 27. jDiameter SL<sub>g</sub> PLA example (sample containing all AVPs executed).

```

23:53:31,764 INFO [ClientLRR] Sending Request: 8388621 [E2E:1370488836 -- HBH:1693543583 -- AppID:16777255]
23:53:31,764 INFO [ClientLRR] Request AVPs:
23:53:31,764 INFO [ClientLRR] <avp name="Session-Id" code="263" vendor="0" value="127.0.0.1;343;3841024432;xx-SLg-TESTxx" />
23:53:31,764 INFO [ClientLRR] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0" />
23:53:31,764 INFO [ClientLRR] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
23:53:31,764 INFO [ClientLRR] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
23:53:31,764 INFO [ClientLRR] </avp>
23:53:31,764 INFO [ClientLRR] <avp name="Destination-Realm" code="293" vendor="0" value="server.mobicens.org" />
23:53:31,764 INFO [ClientLRR] <avp name="Origin-Realm" code="296" vendor="0" value="client.mobicens.org" />
23:53:31,764 INFO [ClientLRR] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
23:53:31,765 INFO [ClientLRR] <avp name="Origin-Host" code="264" vendor="0" value="aaa:/127.0.0.1:13868" />
23:53:31,765 INFO [ClientLRR] <avp name="Location-Event" code="2518" vendor="10415" value="4" />
23:53:31,765 INFO [ClientLRR] <avp name="LCS-EPS-Client-Name" code="2501" vendor="10415" />
23:53:31,765 INFO [ClientLRR] <avp name="LCS-Name-String" code="1238" vendor="10415" value="Restcomm Geolocation API" />
23:53:31,765 INFO [ClientLRR] <avp name="LCS-Format-Indicator" code="1237" vendor="10415" value="2" />
23:53:31,765 INFO [ClientLRR] </avp>
23:53:31,765 INFO [ClientLRR] <avp name="3GPP-IMS" code="1" vendor="10415" value="748039876543210" />
23:53:31,765 INFO [ClientLRR] <avp name="MMSI-MN" code="701" vendor="10415" value="5989907931" />
23:53:31,765 INFO [ClientLRR] <avp name="IMEI" code="1402" vendor="10415" value="011714004661057" />
23:53:31,765 INFO [ClientLRR] <avp name="Location-Estimate" code="1242" vendor="10415" value="N43°38'19.39" W116°14'28.86" />
23:53:31,765 INFO [ClientLRR] <avp name="Accuracy-Fulfilment-Indicator" code="2513" vendor="10415" value="0" />
23:53:31,765 INFO [ClientLRR] <avp name="Age-Of-Location-Estimate" code="2514" vendor="10415" value="37" />
23:53:31,765 INFO [ClientLRR] <avp name="Velocity-Estimate" code="2515" vendor="10415" value="200mph" />
23:53:31,765 INFO [ClientLRR] <avp name="EUTRAN-Positioning-Data" code="2516" vendor="10415" value="eNB453ltea23" />
23:53:31,765 INFO [ClientLRR] <avp name="ECGI" code="2517" vendor="10415" value="eNB9437" />
23:53:31,765 INFO [ClientLRR] <avp name="GERAN-Positioning-Info" code="2524" vendor="10415" />
23:53:31,765 INFO [ClientLRR] <avp name="GERAN-Positioning-Data" code="2525" vendor="10415" value="BT943RNC" />
23:53:31,765 INFO [ClientLRR] <avp name="GERAN-GANSS-Positioning-Data" code="2526" vendor="10415" value="BT943RNC1Ganss43" />
23:53:31,765 INFO [ClientLRR] </avp>
23:53:31,765 INFO [ClientLRR] <avp name="Cell-Global-Identity" code="1604" vendor="10415" value="9342784713907" />
23:53:31,765 INFO [ClientLRR] <avp name="UTRAN-Positioning-Info" code="2527" vendor="10415" />
23:53:31,765 INFO [ClientLRR] <avp name="UTRAN-Positioning-Data" code="2528" vendor="10415" value="NB943RNC1" />
23:53:31,765 INFO [ClientLRR] <avp name="UTRAN-GANSS-Positioning-Data" code="2529" vendor="10415" value="NB031RNC1Ganss43" />
23:53:31,765 INFO [ClientLRR] </avp>
23:53:31,765 INFO [ClientLRR] <avp name="Service-Area-Identity" code="1607" vendor="10415" value="service-area-umts-3" />
23:53:31,765 INFO [ClientLRR] <avp name="LCS-Service-Type-ID" code="2520" vendor="10415" value="234" />
23:53:31,765 INFO [ClientLRR] <avp name="LCS-Service-Sub-Type-ID" code="2521" vendor="10415" value="0" />
23:53:31,765 INFO [ClientLRR] <avp name="LCS-QoS-Class" code="2523" vendor="10415" value="1" />
23:53:31,765 INFO [ClientLRR] <avp name="Servng-Node" code="2401" vendor="10415" />
23:53:31,765 INFO [ClientLRR] <avp name="SGSN-Number" code="1489" vendor="10415" value="59899004501" />
23:53:31,765 INFO [ClientLRR] <avp name="SGSN-Name" code="2409" vendor="10415" value="SGSN01" />
23:53:31,765 INFO [ClientLRR] <avp name="SGSN-Realm" code="2410" vendor="10415" value="sgsn.restcomm.com" />
23:53:31,765 INFO [ClientLRR] <avp name="MME-Name" code="2402" vendor="10415" value="MME710" />
23:53:31,765 INFO [ClientLRR] <avp name="MME-Realm" code="2408" vendor="10415" value="mme.restcomm.com" />
23:53:31,766 INFO [ClientLRR] <avp name="MSC-Number" code="2403" vendor="10415" value="59899001207" />
23:53:31,766 INFO [ClientLRR] <avp name="3GPP-AAA-Server-Name" code="318" vendor="10415" value="aaa.restcomm.com" />
23:53:31,766 INFO [ClientLRR] <avp name="LCS-Capabilities-Set" code="2404" vendor="10415" value="99900123" />
23:53:31,766 INFO [ClientLRR] <avp name="GMLC-Address" code="2405" vendor="10415" value="fe80:f55e:a6df:e4e1:dbb1%21" />
23:53:31,766 INFO [ClientLRR] </avp>
23:53:31,766 INFO [ClientLRR] <avp name="LRR-Flags" code="2530" vendor="10415" value="0" />
23:53:31,766 INFO [ClientLRR] <avp name="LCS-Reference-Number" code="2531" vendor="10415" value="579" />
23:53:31,766 INFO [ClientLRR] <avp name="Deferred-MT-LR-Data" code="2547" vendor="10415" />
23:53:31,766 INFO [ClientLRR] <avp name="Deferred-Location-Type" code="2532" vendor="10415" value="8" />
23:53:31,766 INFO [ClientLRR] <avp name="Termination-Cause" code="2548" vendor="10415" value="7" />
23:53:31,766 INFO [ClientLRR] </avp>
23:53:31,766 INFO [ClientLRR] <avp name="GMLC-Address" code="2405" vendor="10415" value="fe80:f55e:a6df:e4e1:dbb1%21" />
23:53:31,766 INFO [ClientLRR] <avp name="Periodic-LDR-Info" code="2540" vendor="10415" />
23:53:31,766 INFO [ClientLRR] <avp name="Reporting-Amount" code="2541" vendor="10415" value="8639910" />
23:53:31,766 INFO [ClientLRR] <avp name="Reporting-Interval" code="2542" vendor="10415" value="8639998" />
23:53:31,766 INFO [ClientLRR] </avp>
23:53:31,766 INFO [ClientLRR] <avp name="EMMLC-Cell-Info" code="2552" vendor="10415" />
23:53:31,766 INFO [ClientLRR] <avp name="ECGI" code="2517" vendor="10415" value="eNB9437" />
23:53:31,766 INFO [ClientLRR] <avp name="Cell-Portion-ID" code="2553" vendor="10415" value="34923" />
23:53:31,766 INFO [ClientLRR] </avp>
23:53:31,766 INFO [ClientLRR] <avp name="IxrTT-RCI" code="2554" vendor="10415" value="00000010" />
23:53:31,766 INFO [ClientLRR] <avp name="Civic-Address" code="2556" vendor="10415" value="<CivicAddress xml:lang="en-GB" xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
xmlns:cdc="http://devon.canalis.example.com/civic">
<country>UK</country>
<AI>Devon</AI>
<3DMonkokohampton</A3>
<RD>Deekport</RD>
<ST>Cross</ST>
</CivicAddress>
</cdc:bridge>21451338</cdc:bridge>
</CivicAddress>" />
23:53:31,766 INFO [ClientLRR] <avp name="Barometric-Pressure" code="2557" vendor="10415" value="0" />

```

Figure F - 28. jDiameter SLg LRR example (sample containing all AVPs executed).

```

23:53:33,800 INFO [ServerLRA] Sending Answer: 8388621 [E2E:1370488836 -- HBH:1693543583 -- AppID:16777255]
23:53:33,800 INFO [ServerLRA] Request AVPs:
23:53:33,800 INFO [ServerLRA] <avp name="Session-Id" code="263" vendor="0" value="127.0.0.1;343;3841024432;xx-SLg-TESTxx" />
23:53:33,800 INFO [ServerLRA] <avp name="Vendor-Specific-Application-Id" code="260" vendor="0" />
23:53:33,801 INFO [ServerLRA] <avp name="Vendor-Id" code="266" vendor="0" value="10415" />
23:53:33,801 INFO [ServerLRA] <avp name="Auth-Application-Id" code="258" vendor="0" value="16777255" />
23:53:33,801 INFO [ServerLRA] </avp>
23:53:33,801 INFO [ServerLRA] <avp name="Result-Code" code="268" vendor="0" value="2001" />
23:53:33,801 INFO [ServerLRA] <avp name="Auth-Session-State" code="277" vendor="0" value="1" />
23:53:33,801 INFO [ServerLRA] <avp name="GMLC-Address" code="2405" vendor="10415" value="fe80:f55e:a6df:e4e1:dbb1%21" />
23:53:33,801 INFO [ServerLRA] <avp name="LRA-Flags" code="2549" vendor="10415" value="0" />
23:53:33,801 INFO [ServerLRA] <avp name="Reporting-PLMN-List" code="2543" vendor="10415" />
23:53:33,801 INFO [ServerLRA] <avp name="Visited-PLMN-Id" code="1407" vendor="10415" value="74803, 74801" />
23:53:33,801 INFO [ServerLRA] <avp name="Periodic-Location-Support-Indicator" code="2550" vendor="10415" value="1" />
23:53:33,801 INFO [ServerLRA] <avp name="Prioritized-List-Indicator" code="2551" vendor="10415" value="0" />
23:53:33,801 INFO [ServerLRA] </avp>
23:53:33,801 INFO [ServerLRA] <avp name="PLMN-ID-List" code="2544" vendor="10415" />
23:53:33,801 INFO [ServerLRA] <avp name="Visited-PLMN-Id" code="1407" vendor="10415" value="74803, 74801" />
23:53:33,801 INFO [ServerLRA] <avp name="Periodic-Location-Support-Indicator" code="2550" vendor="10415" value="1" />
23:53:33,801 INFO [ServerLRA] </avp>
23:53:33,801 INFO [ServerLRA] <avp name="LCS-Reference-Number" code="2531" vendor="10415" value="579" />
23:53:33,801 INFO [ServerLRA] <avp name="Origin-Host" code="264" vendor="0" value="127.0.0.1" />
23:53:33,801 INFO [ServerLRA] <avp name="Origin-Realm" code="296" vendor="0" value="server.mobicens.org" />

```

Figure F - 29. jDiameter SLg LRA example (sample containing all AVPs executed).





## **Annex G**

### **G Evaluation**

#### **G.1 Qualitative Surveys Guidelines**

The guidelines provided to the evaluators are provided next, identical as they received it (answers are provided in following sections). Following surveys/questionnaires are placed in chronological order, as per the date they were submitted (copied here in the exact format as received).

In the first place, we would like to thank you for participating in this qualitative survey as defined by DESMET methodology [100], consisting of a feature-based evaluation done by experts or people who have had experience of using the method/tool, or have studied the method/tool. As you qualify in that category, we are kindly asking you to proceed with the guidelines to be described next, in order to completing the questionnaire that follows.

This qualitative survey is divided in two stages, comprising two aspects of assessment for answering the questionnaire: 1) Documentation evaluation, 2) Software testing.

The documentation you are kindly asked to assess is given by RestComm Geolocation API and RCML guides [E6-E7] as well as RestComm GMLC Admin Guide [E8].

For the second aspect of this qualitative survey, binaries have been provided to you. Then, you are asked to carry out tests as the ones provided by the examples in [E6] for RestComm Geolocation API software behaviour evaluation. As you are already familiar with running RestComm-Connect, please do it binding to the IP address of your server in case you want to conduct HTTP queries to that IP

(otherwise, you must convey the HTTP queries to loopback IP address, i.e. 127.0.0.1).

Regarding RestComm GMLC testing, please proceed as described in chapter 3 in RestComm GMLC Admin Guide [E8] for simulator mode. You are already familiar with this procedure, but in any case, the aforementioned documentation gives you a step by step guide on how to proceed, including graphics of what the simulator should show you. As described also in [E8], you may find handy to use Wireshark tool in parallel.

The following questionnaire provides you interrogations accordingly to the procedures you followed. Please provide the answer for each question with an X behind the option you consider appropriate, i.e. Fully disagree, Disagree, Neutral, Agree or Fully Agree. In the observations box, you may provide further comments regarding your answer.

1. RestComm Geolocation API design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

2. RestComm Geolocation RCML design, definition and documentation is fully comprehensible and effectively applies for RestComm Visual Designer implementation of Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

3. RestComm Geolocation API effectively provides a user-friendly tool for easily building Location Based Services				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

4. RestComm Geolocation API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

5. RestComm Geolocation API provides adequate means for Web developers to request location information (i.e. cURL).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

6. RestComm Geolocation API provides appropriate format for Web developers to gather location information (i.e. XML or JSON).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

7. RestComm Geolocation API effectively gathers a comprehensive set of immediate or event driven location information				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

8. RestComm Geolocation API effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

9. RestComm GMLC effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

10. RestComm GMLC effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

11. RestComm GMLC effectively provides Carrier Grade performance as for [E9].				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

12. RestComm GMLC effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed)				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

13. RestComm jDiameter implementation of SLh and SLg interfaces for LTE location services as for 3GPP TS 29.172/29.173 [44-45] effectively complies with the needs of gathering location services from an LTE network being them embedded in RestComm GMLC, and the former complies with 3GPP/LTE specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed)				
Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

14. RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.

Fully disagree	Disagree	Neutral	Agree	Fully agree
Observations				

Additional comments:

Name: \_\_\_\_\_

Email: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

As stated earlier, following sections provide surveys/questionnaires in chronological order as they were submitted. Digital copies of the entire documents are embedded here:



## G.2 Qualitative Survey of Jean Deruelle

1. RestComm Geolocation API design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	The documentation has been available online at <a href="http://documentation.telestax.com/connect/api/geolocation-api.html">http://documentation.telestax.com/connect/api/geolocation-api.html</a> and vetted by the open source community and partners.			

2. RestComm Geolocation RCML design, definition and documentation is fully comprehensible and effectively applies for RestComm Visual Designer implementation of Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	The documentation has been available online at <a href="http://documentation.telestax.com/connect/rcml/geolocation-rcml.html">http://documentation.telestax.com/connect/rcml/geolocation-rcml.html</a> and vetted by the open source community and partners.			

3. RestComm Geolocation API effectively provides a user-friendly tool for easily building Location Based Services				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

4. RestComm Geolocation API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X

Observations	The goal was met of having an API which was not biased by Telecom terms and more inline with natural understanding of non experts akin to Google and Apple APIs on Mobile so users would stay in a world they already know to get a faster time to market to build innovation services including GeoLocation
--------------	--

5. RestComm Geolocation API provides adequate means for Web developers to request location information (i.e. cURL).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

6. RestComm Geolocation API provides appropriate format for Web developers to gather location information (i.e. XML or JSON).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

7. RestComm Geolocation API effectively gathers a comprehensive set of immediate or event driven location information				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

8. RestComm Geolocation API effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

9. RestComm GMLC effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X



Observations	It has been deployed successfully in customer real world deployments
--------------	--

10. RestComm GMLC effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

11. RestComm GMLC effectively provides Carrier Grade performance as for [E9].				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	It has been tested at more than 1500 requests per second successfully			

12. RestComm GMLC effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed)				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	It has been deployed successfully in customer real world deployments			

13. RestComm jDiameter implementation of SLh and SLg interfaces for LTE location services as for 3GPP TS 29.172/29.173 [44-45] effectively complies with the needs of gathering location services from an LTE network being them embedded in RestComm GMLC, and the former complies with 3GPP/LTE specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed)				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X

Observations	
--------------	--

14. RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

Additional comments:

Name: Jean Deruelle

Email: jean.deruelle@telestax.com

Date: 04/11/2016

Signature: \_\_\_\_\_



## G.3 Qualitative Survey of Andrew Eross

1. RestComm Geolocation API design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	<p>The online documentation for the system is well structured and extensive:  <a href="http://documentation.telestax.com/connect/api/geolocation-api.html">http://documentation.telestax.com/connect/api/geolocation-api.html</a></p> <p>The documentation structure was discussed and revised with input from several industry partners (including myself):  <a href="https://groups.google.com/forum/#!topic/restcomm/meSloxn5tfQ">https://groups.google.com/forum/#!topic/restcomm/meSloxn5tfQ</a></p>			

2. RestComm Geolocation RCML design, definition and documentation is fully comprehensible and effectively applies for RestComm Visual Designer implementation of Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	<p>The online documentation for this component is also extensive and complete:  <a href="http://documentation.telestax.com/connect/rcml/geolocation-rcml.html">http://documentation.telestax.com/connect/rcml/geolocation-rcml.html</a></p>			

3. RestComm Geolocation API effectively provides a user-friendly tool for easily building Location Based Services				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	<p>The documentation is clear, the tool is effective, and the service works well.</p>			

4. RestComm Geolocation API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	The API design was created specifically to be thorough, but uncluttered by the excessive complexity of the underlying protocols. It is fully abstracted from the underlying components (e.g. the GMLC in this case).			

5. RestComm Geolocation API provides adequate means for Web developers to request location information (i.e. cURL).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the API is RESTful and could easily be accessed via standard web API development tools (cURL, Postman, etc).			

6. RestComm Geolocation API provides appropriate format for Web developers to gather location information (i.e. XML or JSON).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the API supports both standard XML/JSON.			

7. RestComm Geolocation API effectively gathers a comprehensive set of immediate or event driven location information				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the API has support for "Immediate" and "Notification" location data requests for precisely this purpose.			

8. RestComm Geolocation API effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the API is specifically designed to use OMA MLP to communicate to the back-end GMLC.			

9. RestComm GMLC effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.				
Fully disagree	Disagree	Neutral	Agree	Fully agree

				X
Observations	Yes, the GMLC supports both legacy and NextGen networks and has been deployed in these environments.			

10. RestComm GMLC effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the GMLC supports both simple HTTP REST and also OMA MLP requests.			

11. RestComm GMLC effectively provides Carrier Grade performance as for [E9].				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the underlying architecture platform has been tested for years in real-world carrier environments, and the GMLC itself has been load tested at high TPS levels.			

12. RestComm GMLC effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed)				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the GMLC has been deployed in real-world environments and tested for both 2G and 3G location. My company has successfully deployed the GMLC within a Hong Kong based carrier and utilized it for these purposes.			

13. RestComm jDiameter implementation of SLh and SLg interfaces for LTE location services as for 3GPP TS 29.172/29.173 [44-45] effectively complies with the needs of gathering location services from an LTE network being them embedded in RestComm GMLC, and the former complies with 3GPP/LTE				
---	--	--	--	--

specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed)				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

14. RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes, the solution is scalable, load tested, supports both synchronous and asynchronous access modes, and can be utilized for these access scenarios.			

Additional comments:

Name: Andrew Eross

Email: eross@locatrix.com

Date: 10/11/2016

Signature: 

## G.4 Qualitative Survey of Marcelo Aranibar

1. RestComm Geolocation API design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

2. RestComm Geolocation RCML design, definition and documentation is fully comprehensible and effectively applies for RestComm Visual Designer implementation of Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

3. RestComm Geolocation API effectively provides a user-friendly tool for easily building Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

4. RestComm Geolocation API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				



5. RestComm Geolocation API provides adequate means for Web developers to request location information (i.e. cURL).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

6. RestComm Geolocation API provides appropriate format for Web developers to gather location information (i.e. XML or JSON).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

7. RestComm Geolocation API effectively gathers a comprehensive set of immediate or event driven location information.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

8. RestComm Geolocation API effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

9. RestComm GMLC effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

10. RestComm GMLC effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

11. RestComm GMLC effectively provides Carrier Grade performance as for [E9].				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

12. RestComm GMLC effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

13. RestComm jDiameter implementation of SLh and SLg interfaces for LTE location services as for 3GPP TS 29.172/29.173 [44-45] effectively complies with the needs of gathering location services from an LTE network being them embedded in RestComm GMLC, and the former complies with 3GPP/LTE specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

14. RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

Additional comments:

Name: MARCELO ARANIBAR

Email: aranibarm@tigo.net.bo

Date: 10/11/2016

Signature: 

## G.5 Qualitative Survey of James Body

### Evaluation Qualitative Surveys

In the first place, we would like to thank you for participating in this qualitative survey as defined by DESMET methodology [100], consisting of a feature-based evaluation done by experts or people who have had experience of using the method/tool, or have studied the method/tool. As you qualify in that category, we are kindly asking you to proceed with the guidelines to be described next, in order to completing the questionnaire that follows. This qualitative survey is divided in two stages, comprising two aspects of assessment for answering the questionnaire: 1) Documentation evaluation, 2) Software testing.

The documentation you are kindly asked to assess is given by RestComm Geolocation API and RCML guides [E6-E7] as well as RestComm GMLC Admin Guide [E8]. For the second aspect of this qualitative survey, binaries have been provided to you. Then, you are asked to carry out tests as the ones provided by the examples in [E6] for RestComm Geolocation API software behaviour evaluation. As you are already familiar with running RestComm-Connect, please do it binding to the IP address of your server in case you want to conduct HTTP queries to that IP (otherwise, you must convey the HTTP queries to loopback IP address, i.e. 127.0.0.1). Regarding RestComm GMLC testing, please proceed as described in chapter 3 in RestComm GMLC Admin Guide [E8] for simulator mode. You are already familiar with this procedure, but in any case, the aforementioned documentation gives you a step by step guide on how to proceed, including graphics of what the simulator should show you. As described also in [E8], you may find handy to use Wireshark tool in parallel.

The following questionnaire provides you interrogations accordingly to the procedures you followed. Please provide the answer for each question with an X behind the option you consider appropriate, i.e. Fully disagree, Disagree, Neutral, Agree or Fully Agree. In the observations box, you may provide further comments regarding your answer.

1.	RestComm Geolocation API design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.				
	Fully disagree	Disagree	Neutral	Agree	Fully agree

				X
Observations	Both design and definition of the API are extremely well documented and are readily available as online resources			

2. RestComm Geolocation RCML design, definition and documentation is fully comprehensible and effectively applies for RestComm Visual Designer implementation of Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	RCML documentation is also well written and is available online			

3. RestComm Geolocation API effectively provides a user-friendly tool for easily building Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
			X	
Observations	As a first iteration the Geolocation API provides a useful user-friendly tool with which LBS applications can be built. Further iterations will add further			

4. RestComm Geolocation API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Underlying protocols are effectively abstracted so as to negate the need for Web developers to have detailed knowledge of their implementation within communications networks			

5. RestComm Geolocation API provides adequate means for Web developers to request location information (i.e. cURL).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

6. RestComm Geolocation API provides appropriate format for Web developers to gather location information (i.e. XML or JSON).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes – both XML and JSON are supported			

7. RestComm Geolocation API effectively gathers a comprehensive set of immediate or event driven location information.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

8. RestComm Geolocation API effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes – the Geolocation API incorporates OMA Mobile Location Protocol (MLP) specifically to provide interconnection with 3 <sup>rd</sup> party GMLCs			

9. RestComm GMLC effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes – by providing an accessible and cost effective interface through which LBS applications can utilise location data			

10. RestComm GMLC effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Compliant with both HTTP and MLP standards			

11. RestComm GMLC effectively provides Carrier Grade performance as for [E9].				
Fully disagree	Disagree	Neutral	Agree	Fully agree
			X	
Observations	I believe this to be correct. This will be proven by first MNO deployments			

12. RestComm GMLC effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Yes – compatible with both 2G and 3G location procedures			

13. RestComm jDiameter implementation of SLh and SLg interfaces for LTE location services as for 3GPP TS 29.172/29.173 [44-45] effectively complies with the needs of gathering location services from an LTE network being them embedded in RestComm GMLC, and the former complies with 3GPP/LTE specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Both SLh and SLg interfaces appear to be implemented as per 3GPP TS 29.172/29.173			

14. RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	This Geolocation API offers a comprehensive range of access methods and is agnostic of UE and RAN vendor type.			

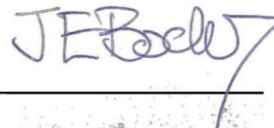
Additional comments:

Name: James Body Head of Research & Development Truphone

Email: james.body@truphone.com

Date: 11<sup>th</sup> November 2016

Signature: \_\_\_\_\_





## G.6 Qualitative Survey of Julio Rey

1. RestComm Geolocation API design, definition and documentation is fully comprehensible for a Web developer with no previous knowledge on the subject.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	<a href="http://documentation.telestax.com/connect/api/geolocation-api.html">http://documentation.telestax.com/connect/api/geolocation-api.html</a> is one of the most remarkable API definitions I have ever read.			

2. RestComm Geolocation RCML design, definition and documentation is fully comprehensible and effectively applies for RestComm Visual Designer implementation of Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	You need to have RCML experience for this one, so it is quite tricky in the beginning.			

3. RestComm Geolocation API effectively provides a user-friendly tool for easily building Location Based Services.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	If you understand the previous one, this one is full compliant.			

4. RestComm Geolocation API effectively complies with providing a SOA approach solution for Web developers with no knowledge of Telecommunication protocols or underlying network topologies.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	I can say I was one of those until training received from Fernando Mendioroz and Charles Roufay from TeleStax in December 2015 at Asunción del Paraguay during one long intense week. The training was outstanding and since then and posterior support from either Fernando or Charles on several queries, I became full capable of understanding Telecommunication protocols or underlying network topologies.			

5. RestComm Geolocation API provides adequate means for Web developers to request location information (i.e. cURL).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Execution of cURL commands like in the examples provided in the API documentation work.			

6. RestComm Geolocation API provides appropriate format for Web developers to gather location information (i.e. XML or JSON).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Similar comment as previous.			

7. RestComm Geolocation API effectively gathers a comprehensive set of immediate or event driven location information.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Event driven location information is a very attractive feature for our business interests.			

8. RestComm Geolocation API effectively interacts with RestComm GMLC or is already set to connect with third party GMLCs that comply with 3GPP/LTE and OMA specifications.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	As for what I comment in 4 and 10, I can fully agree with this statement.			

9. RestComm GMLC effectively complies with latest trends for retrieving location information either in legacy or Next Generation Networks.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Same as previous.			

10. RestComm GMLC effectively complies with the needs of a GMLC client using HTTP (GET/POST) and OMA MLP [107] procedures.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	During TADHack Uruguay (May 2016), Fernando Mendioroz and Andrew Eross instructed me on OMA MLP. GMLC was already compliant with MLP by then, as they showed me examples that worked.			

11. RestComm GMLC effectively provides Carrier Grade performance as for [E9].				
Fully disagree	Disagree	Neutral	Agree	Fully agree
			X	
Observations	As for [E9] I agree, however we need to further test with full capable operators (something we are looking forward to do).			

12. RestComm GMLC effectively complies with 3GPP specifications for gathering location information in GSM or UMTS in Circuit-Switched Core Networks and 2G or 3G Radio Access Networks if these comply with 3GPP specifications in that regard (i.e. SMLC and positioning methods like OTDOA are placed).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

13. RestComm jDiameter implementation of SLh and SLg interfaces for LTE location services as for 3GPP TS 29.172/29.173 [44-45] effectively complies with the needs of gathering location services from an LTE network being them embedded in RestComm GMLC, and the former complies with 3GPP/LTE specifications in that regard (i.e. E-SMLC and positioning methods like OTDOA are placed).				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations				

14. RestComm Geolocation API and RestComm GMLC comprise a complete but yet scalable solution for providing Location Based Services triggered by any kind of asynchronous events, either from the Internet via REST Web Services or MNO messaging services like USSD or SMS and therefore, fulfilling motivational scenarios needs for MFS or emergency services like the ones discussed in [36-38, 105-106], regardless of user equipment and radio access network.				
Fully disagree	Disagree	Neutral	Agree	Fully agree
				X
Observations	Being a senior software engineer and having worked in this area for quite some time now (telecommunications), I can confidently agree with this statement.			

Additional comments: We are presently discussing at commercial level for an agreement between our companies for acquiring the full combo of Restcomm Geolocation API and Restcomm GMLC (we've already worked with other Restcomm solutions for USSD, SMS and voice) as it will provide very interesting value to our services portfolio.

Name: Julio César Rey Méndez

Email: [julio.rey@americanprepaidvas.com](mailto:julio.rey@americanprepaidvas.com)

Date: 12/11/2016



Julio Cesar Rey Mendez

Signature: