NGN/IMS a fondo

PID_00265730

Víctor Huertas García

Tiempo mínimo de dedicación recomendado: 7 horas

Universitat Oberta de Catalunya

Víctor Huertas García

Ingeniero en Telecomunicaciones por la Universitat Politècnica de Catalunya. Actualmente trabaja como ingeniero de *networking* y experto en NGN/IMS en el departamento de Equipos de Comunicación en la multinacional Indra Sistemas. Ha participado en numerosos proyectos de la ESA (Agencia Europea del Espacio) de investigación sobre la aplicación de la tecnología IP en redes satélite. Recientemente ha participado en proyectos de integración de IMS en las redes satélite para conseguir la convergencia con redes terrestres.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Victor Garcia Font

Segunda edición: septiembre 2019
Autoría: Víctor Huertas García

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

El paradigma introducido por las redes NGN posibilita que cualquier red que pueda transmitir paquetes IP se convierta en una red multiservicio con garantía de calidad de servicio. Se produce un total desacoplo entre los servicios ofrecidos a los usuarios y la tecnología de las redes de transporte.

Si ha habido una entidad de estandarización y especificación que ha llevado la voz cantante en la especificación de NGN e IMS esa es 3GPP, focalizándose sobre todo en las redes que más dinero mueven en el mercado de las telecomunicaciones hoy en día, las redes de telefonía móvil. Este módulo se focalizará en el modelo de referencia que esta entidad propone tanto para la **capa de transporte** (LTE) como para la **capa de servicio** (núcleo IMS).

Finalmente, abordaremos la **capa que afecta a las aplicaciones**, que es en realidad lo que aporta valor añadido a los servicios que los usuarios acceden desde sus terminales. En esta área, como veremos, hay más laxitud en cuanto a su especificación ya que se han indicado sus características a más alto nivel. La propia industria es la que ha rellenado los huecos dejados por la especificación proponiendo sus propias soluciones.

En resumen, en este módulo se verán con más detalle todas las capas del modelo de referencia proponiendo ejemplos de cómo hoy en día se han implementado (por ejemplo, en las redes LTE) y cómo su arquitectura ha ido evolucionando según los requerimientos que el propio mercado ha impuesto (por ejemplo, la irrupción de Wi-Fi como tecnología universal de acceso casi a nivel global).

Objetivos

Los contenidos de este módulo han de permitir a los estudiantes los objetivos siguientes:

1. Conocer los bloques funcionales que definen los modelos de referencia del 3GPP y que afectan a las siguientes capas:

   a) Capa de transporte de LTE: *Evolved Packet System* y modelo de referencia PCC para garantía de QoS.
   b) Capa de servicio: núcleo IMS compuesto primordialmente por P-CSCF, I-CSCF y S-CSCF.
   c) Capa de aplicación: integración del núcleo IMS con servidores de aplicación de redes heredadas y SIP.

2. Identificar los puntos de referencia (o interfaces) entre bloques de la capa de transporte y de servicio (núcleo IMS).

3. Identificar y conocer los puntos de referencia (o interfaces) entre el núcleo IMS y la capa de transporte y su importancia en la garantía de QoS extremo a extremo tanto en modo *push* como en modo *pull*.

4. Conocer los principales protocolos empleados en un contexto NGN/IMS para el establecimiento de sesiones multimedia y el control de admisión y recursos: SIP y Diameter.

5. Comprender la filosofía de un servicio NGN y su paralelismo con el paradigma SOA.

6. Conocer la interacción a nivel de interfaces y funcionalidades genéricas en la invocación de servicios en un contexto de IMS para los siguientes actores según el modelo del 3GPP:

   a) Usuario y su interacción directa con el núcleo IMS y con el servidor de aplicación.
   b) El núcleo IMS con el servidor de aplicación.

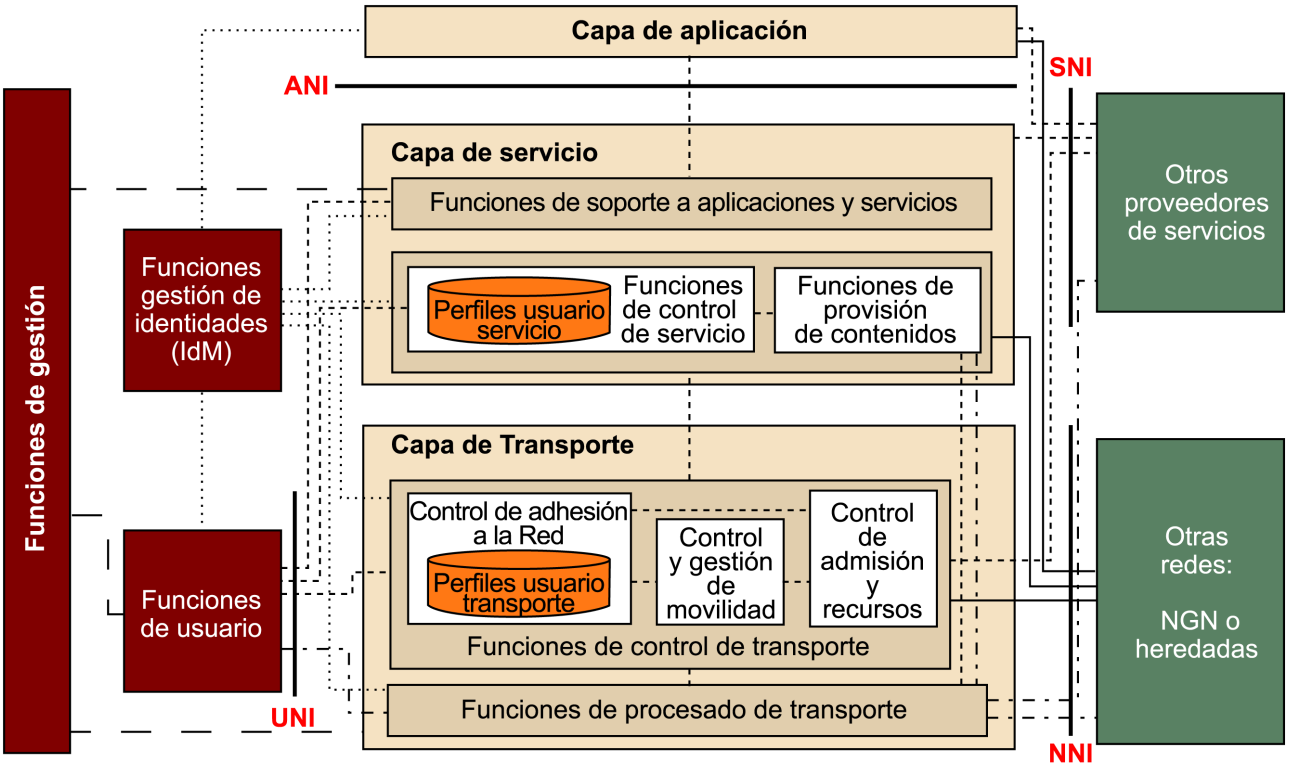
7. Entender la importancia de la orquestación en la integración de servicios.

8. Capacidad para comprender las funcionalidades del *Service Broker* y su arquitectura interna.

1. Arquitectura funcional de NGN / IMS

Las redes de próxima generación o redes NGN se caracterizan por estar basadas íntegramente en paquetes IP y por el acceso libre a servicios multimedia con garantía de calidad de servicio (QoS) extremo a extremo con independencia de la tecnología de la red de transporte (tanto en la red de acceso como troncal).

Figura 1. Arquitectura de referencia según *Release 2* de redes NGN de la ITU-T.



La Figura 1 se corresponde a la *Release 2* de la arquitectura, a la que se han introducido algunos bloques nuevos con respecto al *Release 1*, enfocados básicamente a servicios como IPTV, gestión de identidades y movilidad en la capa de transporte.

A pesar de que la ITU-T ha tenido un papel armonizador de todas las especificaciones que han ido surgiendo a lo largo de los años con respecto a las NGN, al final la industria de la telefonía móvil es la que ha llevado la iniciativa en la evolución futura de dichas especificaciones. Y si hay una entidad que ha contribuido y está contribuyendo a la definición de las redes de telefonía móvil es sin duda el 3GPP; esta es la especificación en la que nos vamos a basar en las próximas secciones.

Así pues, veremos a continuación cada una de las partes y capas que conforman la arquitectura 3GPP de referencia para las redes LTE empezando por la capa de transporte y sus funciones, subiendo hasta la capa de servicio y finalmente a la capa de aplicación.

Antes de abordar la descripción de todas las capas y subcapas de cada modelo, vamos a definir dos conceptos que os vais a encontrar a lo largo de todo el documento.

Entidad funcional

La entidad funcional se define como el concepto lógico que especifica una serie de funciones únicas que no son realizadas por otras entidades funcionales. Las entidades funcionales se pueden agrupar para describir implementaciones físicas y prácticas de las mismas.

Las entidades funcionales que definen la arquitectura genérica de redes NGN son entidades abstractas que se definen de forma más concisa cuando son instanciadas en un contexto concreto tecnológicamente hablando. Es decir, que se podría dar el caso de que una instancia de una entidad funcional tenga un comportamiento ligeramente diferente dependiendo de dicho contexto.

Esto condiciona totalmente la implementación de la interfaz (también llamada punto de referencia) entre dos mismas entidades funcionales y, por lo tanto, la descripción de este sólo tiene sentido cuando conocemos las instancias particulares que se usan en un contexto.

Punto de referencia

El punto de referencia es un punto de unión entre dos entidades funcionales bien diferenciadas. Los puntos de referencia pueden ser usados para identificar el tipo de información que se intercambia entre dichas entidades funcionales. A nivel de implementación física, un punto de referencia se puede corresponder con una o más interfaces físicas entre dos equipos y puede implementarse con protocolos que se adapten al intercambio de dicha información, como puede ser el caso de Diameter.

2. Capa de transporte

El 3GPP es la entidad que ha especificado las tecnologías más importantes en el mundo de la telefonía móvil desde GPRS pasando por UMTS, LTE y acabando con 5G. A continuación, vamos a describir la especificación del 3GPP con respecto a la capa de transporte.

Podemos distinguir dos arquitecturas de referencia que en realidad una está contenida dentro de la otra:

- **EPS (*Evolved Packet System*):** incluye todas las entidades funcionales que definen tanto la red de acceso radio LTE como la red troncal. Estas entidades ofrecen las funcionalidades de control de recursos radio, autenticación de equipos de usuario y el establecimiento de conectividad IP dentro de la red del operador.

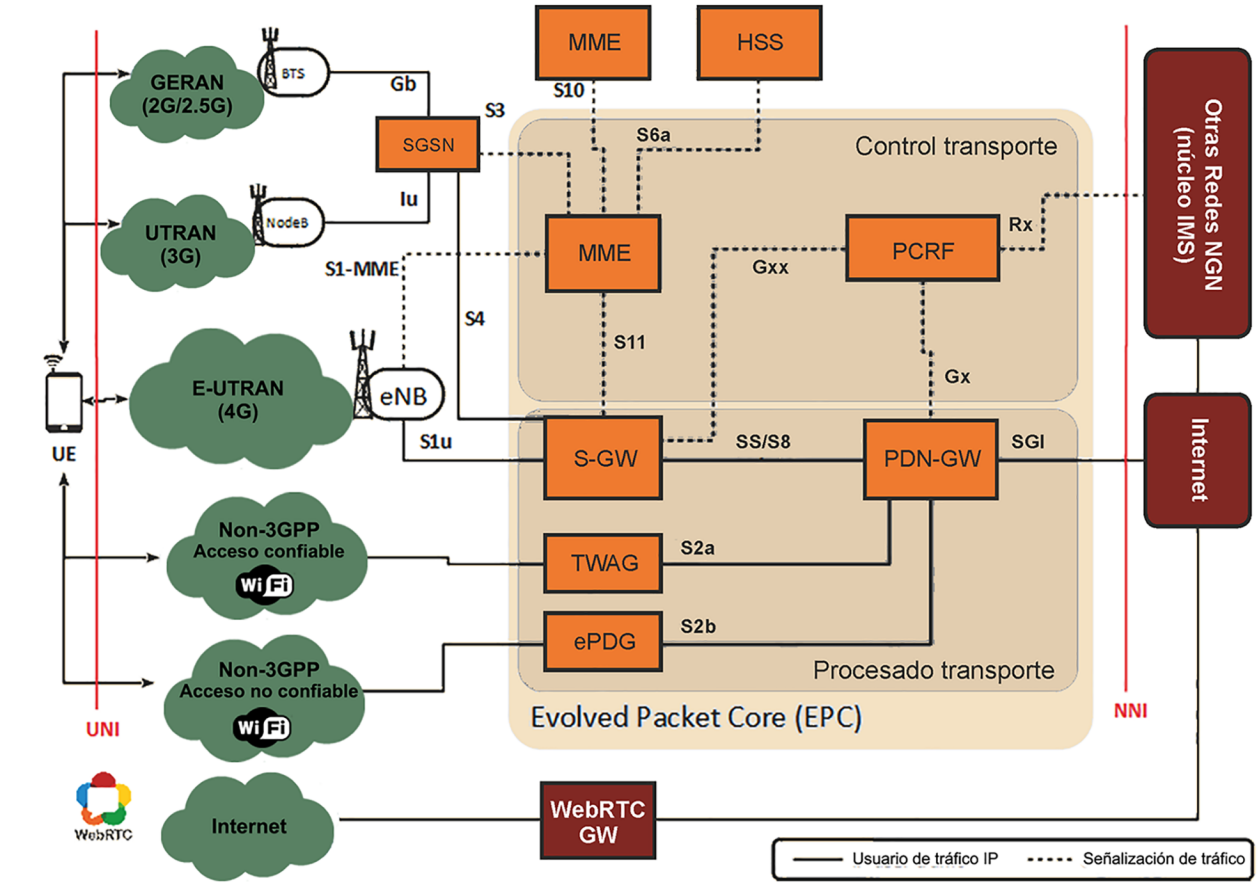
- **PCC (*Policy and Charging Control*):** es un subconjunto del EPS, que tiene la función de aplicar políticas de QoS y controles de facturación de uso de servicios por parte de los usuarios.

2.1. Evolved Packet System

En la Figura 2 se puede apreciar la arquitectura funcional de las redes de acceso y troncal de LTE que 3GPP propone, el cual es llamado *Evolved Packet System*.

El ***Evolved Packet System*** es la suma de dos subconjuntos: el **E-UTRAN** (*Evolved UMTS Terrestrial Radio Access Network*) en la parte de red de acceso radio y el **EPC** (*Evolved Packet Core*) en la parte de la red troncal.

Figura 2. Arquitectura de referencia del *Evolved Packet System.*



En la Figura 2 también podemos ver cómo otras redes definidas por el 3GPP se integran con el EPS como son las redes de acceso 2G y 3G, así como redes que se llaman de *mobile offload*, que primordialmente son redes Wi-Fi o femtoceldas en interiores de edificios.

Mobile offload

Las redes Wi-Fi, al estar integradas en el EPC, actúan como si fuera una extensión de la cobertura en interior de edificios o incluso en el extranjero a modo de *roaming*.

Todas estas redes inalámbricas tan diversas deben integrarse en una red troncal de LTE porque el equipo de usuario (UE) las posee integradas también, pudiéndolas usar en todo momento según su ubicación y el nivel de cobertura que tenga de cada una. Consecuentemente habrá ocasiones en que se deberá realizar un *handover* transparente (sin cortes en la sesión de servicio) de una red a otra y deberá existir cierta coordinación de traspaso de sesión entre estas redes de acceso y aquí el EPC tiene un papel muy importante.

Así pues, veremos primero los elementos principales que forman la arquitectura EPS para posteriormente, en la sección 2.2, ver el modelo de referencia PCC (*Policy and Charging Control*).

Introducción al *Evolved Packet System*

La Figura 2 muestra la arquitectura del EPS o también llamado SAE (*System Architecture Evolution*) cuyas entidades funcionales veremos a continuación.

Comenzamos por la parte del **equipo de usuario** (UE). El equipo de usuario en una red de comunicaciones móviles LTE equivale a un terminal único portátil que, como hemos mencionado antes, es compatible con múltiples generaciones de redes de telefonía móvil, así como Wi-Fi.

A continuación del UE está la red de acceso radio de LTE, que se llama **E-UTRAN**. Dicha red de acceso radio (basado en OFDMA) acaba en el eNodeB (Evolved Node B) que, para que nos entendamos, es la estación base de LTE. Este elemento establece una serie de canales virtuales radio con cada equipo de usuario y dichos canales tienen particularidades que afectan a la garantía de QoS. Los paquetes IP se mapean en estos canales virtuales, también llamados en inglés *radio bearers*.

OFDMA

Método de acceso que permite asignar un número diferente de subportadoras a cada uno de los usuarios garantizando así, una diferente calidad de servicio (QoS) en función del ancho de banda asignado.

El siguiente elemento, ya dentro del EPC, es el **SGW** (*Service Gateway*) y está exclusivamente relacionado con el mecanismo de movilidad. Si un equipo de usuario se desplaza de una celda a otra (dentro de LTE), el eNodeB asociado cambia, pero no el SGW, el cual está considerado como una pasarela de anclaje en el servicio de movilidad.

Interfaz S4

La interfaz entre el SGSN y la SGW se denomina interfaz S4. Proporciona soporte de plano de usuario para servicio de movilidad entre el núcleo GPRS y la SGW. También habilita a la SGW para anclar el traspaso intra-3GPP (TS 23.401).

Si, por ejemplo, el usuario se desplaza a una zona donde hay exclusivamente cobertura de 2G el SGW se coordinará con la SGSN (*Service GPRS Support Node*) a través de la cual haría llegar el tráfico de usuario (vía la interfaz S4).

En este servicio de movilidad cabe destacar otro elemento muy importante: el **MME** o ***Mobility Management Entity***. Este elemento no procesa paquetes de usuario, sino que realiza tareas de control de movilidad dentro de las redes 3GPP incluyendo redes de acceso de otras generaciones como UTRAN (3G) o GERAN (2G). Para ello se coordina con el SGSN vía una interfaz de control llamada S3. Un MME puede también coordinarse con otros MMEs que controlan otros clústeres de eNodeBs adyacentes y así facilitar el *handover* dentro de la red de acceso radio LTE. Para ello se usa la interfaz de control S10.

SGSN

El SGSN es un nodo que encamina sesiones de datos, como conectividad a Internet vía GPRS. Estas sesiones o llamadas de datos son referidas generalmente como de ámbito *Packet Switched* o conmutación de paquetes ya que transportan paquetes IP.

El MME realiza otras funciones. Por ejemplo, asigna al UE el SGW en el que anclarse en el momento en que éste se adhiere a la red radio (al encenderse).

Interfaz S3

La conexión SGSN/MME es proporcionada por la interfaz S3. Permite el intercambio de información para la movilidad entre las redes de acceso 3GPP (TS 23.401).

El MME también aglutina información actualizada de localización de cada equipo de usuario, tal como a qué eNodeB está asociado. Esto es importante cuando se produce una llamada entrante hacia un usuario y hay que localizarlo a nivel de celda (al servicio de localización se le llama *paging*). El MME también realiza tareas de autenticación del equipo de usuario en el momento

en que se produce la adhesión a la red. Por eso el MME tiene un punto de referencia dedicado (S6a) de interconexión al HSS (*Home Subscriber Server*), donde se almacena la información de credenciales del usuario y perfil de suscripción a nivel de transporte (el HSS también almacena información de perfil a nivel de control de servicio). La descripción en detalle de este servicio se abordará en la sección 3 donde se describe el núcleo IMS).

Finalmente, el MME también participa en tareas de gestión de *radio bearers* (como en la activación y desactivación de estos).

Las redes 3GPP

Las redes 3GPP se consideran no solo las celdas de un sistema LTE sino también incluye redes GPRS y UMTS, cuyas tareas de movilidad también las asume el MME a través de puntos de referencia dedicados que le unen con los nodos de estas redes de acceso radio (GERAN para GPRS y UTRAN para UMTS).

Para finalizar tenemos el último elemento del EPC, el **PDN GW**.

Interfaz S6a

La interfaz entre MME y HSS es el S6a. Se utiliza para la transferencia de información de suscripción, autenticación y autorización de usuarios (TS 23.401).

El **PDN GW o *Packet Data Network Gateway***es el elemento fronterizo del sistema EPS con otras redes externas como Internet o IMS. De hecho, la configuración típica en un EPC es tener un PDN GW por cada APN (*Access Point Name*) y normalmente se tiene un APN para la interconexión a Internet y otro APN para la interconexión con el núcleo IMS (dos PDN GW en total).

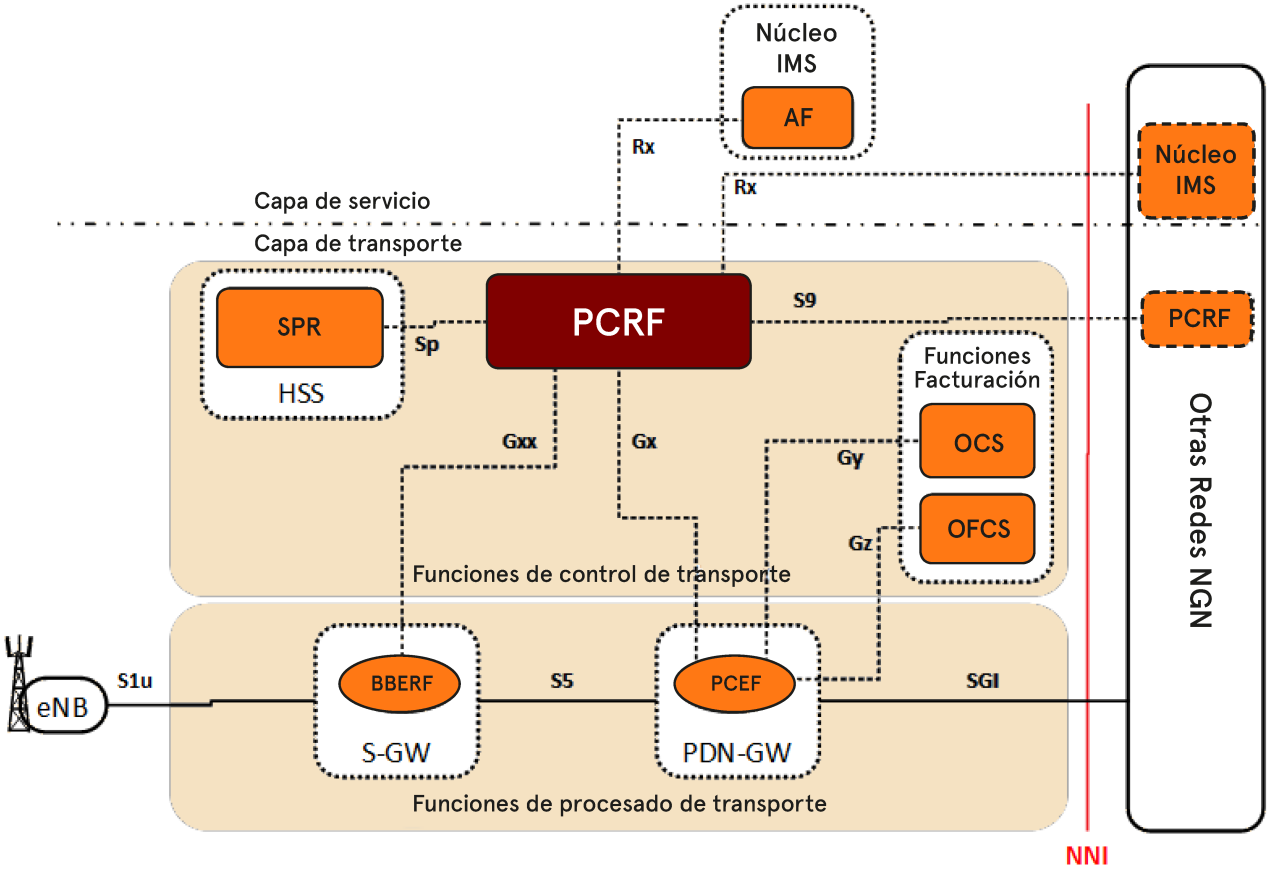
Este elemento juega un papel muy importante en la garantía de QoS, como veremos más adelante, y también se encarga de asignar las direcciones IP a los equipos de usuario.

Se asigna una IP por PDN GW, así que si un usuario es suscriptor de un servicio de datos (Internet) y además de servicios de IMS (VoLTE), al estar conectado a dos PDN GWs distintas a la vez, tendrá asignadas dos direcciones IPs: una la usará para el servicio de Internet y la otra para servicios multimedia IMS (señalización IMS y tráfico de voz/video).

2.2. QoS en LTE: el modelo de referencia de PCC

Ahora que hemos visto la estructura básica del sistema EPS que 3GPP define para LTE, vamos a definir varios conceptos clave para entender cómo se gestiona la QoS en la arquitectura de referencia de PCC (ver Figura 3).

Figura 3. Arquitectura de referencia del PCC.



El PCC trabaja a nivel de flujos de datos de servicios o SDFs (*Service Data Flows*) y proporciona funciones para el control de políticas y de facturación (cargos monetarios asociados) así como reporte de eventos para los SDFs.

La funcionalidad del PCC se resume en dos puntos principales:

1) Control de facturación en base a flujos: en los que se encuentran el control de cargos monetarios asociados y el control de crédito *online*.

2) Control de políticas: en los que se encuentran principalmente el control de acceso a la red y control de la QoS de los servicios invocados (por ejemplo, conectividad a Internet y VoLTE, entre otros).

Cada SDF viene asociado a una **regla de PCC** y puede estar sujeto a control de políticas, a control de facturación o a los dos a la vez.

Una **regla PCC** está definida por el PCRF tras tomar la decisión de control de admisión de la solicitud de recursos de servicio recibida tanto desde la interfaz Rx (llamado modo *push* cuando se recibe desde el AF o *Application Function*) como desde la interfaz Gx (llamado modo *pull* cuando se recibe desde la PDN-GW). Esta **regla PCC** está compuesta por los siguientes parámetros:

- **Nombre de regla** (identificador único).
- **Identificador de servicio o SDF**: Es un valor entero que identifica un servicio o componente de servicio.
- **Filtro(s) IP asociados a los SDF**: Cada filtro fija parámetros de la cabecera del paquete TCP/IP para mapear el tráfico real a un SDF.
- **Precedencia:** orden de aplicación del filtro o filtros.
- **Estatus de acceso:** abierto o cerrado, dejar o no dejar pasar el tráfico asociado.
- **Parámetros QoS:** contiene QCI, ARP y velocidad de bit para subida y bajada.
- **Clave de facturación** (en inglés, *rating group*) **y otros parámetros de facturación**: usados para facturación *online* y *offline*.
- **Clave de monitorización**

Interfaz Rx

La interfaz entre PCRF y AF (*Application Function*) es el Rx. Utilizada por el AF para la solicitud de recursos de QoS y reporte de eventos de capa de transporte. El 3GPP recomienda el protocolo Diameter para su implementación (TS 29.214).

Interfaz Gx

La interfaz entre PCRF y PCEF es el Gx. Utilizada por el PCRF para instalar las reglas PCC (establecimiento de *IP-CAN bearer* y asignación de flujos de datos de servicio). También usado para reporte de eventos de capa de transporte. El 3GPP recomienda el protocolo Diameter para su implementación (TS 29.212).

IP-CAN

Responde a las siglas en inglés de *IP-Connectivity Access Network*.

El PCC asocia la información de servicio y la de transporte de tal manera que la facturación y las políticas quedan totalmente ligadas de cara a integrar redes de transporte heterogéneas. De hecho, relaciona una sesión a nivel de servicio (asociada a la interfaz Rx) con una sesión IP-CAN a nivel de transporte (asociada a la interfaz Gx/Gxx).

El 3GPP define una **sesión IP-CAN** (o también llamada **sesión EPS** si la red de acceso es LTE) como la asociación entre el equipo de usuario (UE) y una red de acceso IP cualquiera. Una sesión IP-CAN puede incorporar una agrupación de uno o más túneles IP-CAN llamados también *IP-CAN bearers (EPS bearers* si la red es LTE). Una sesión IP-CAN está presente siempre que haya una dirección IP asignada al UE y notificada a la red de acceso IP. Así que, si un UE está asociado a dos APNs en una red LTE, tendrá dos direcciones IP asignadas y por lo tanto tendrá dos sesiones EPS activas simultáneamente con los respectivos túneles establecidos.

Interfaz Gxx

La interfaz entre PCRF y BBERF es el Gxx. Utilizada por el PCRF para instalar las reglas PCC (establecimiento de *IP-CANbearer* y asignación de flujos de datos de servicio). También usado para reporte de eventos de capa de transporte. El 3GPP recomienda el protocolo Diameter para su implementación (TS 29.212).

A continuación, describiremos las entidades funcionales que conforman el modelo arquitectural PCC y lo haremos primero abordando la subcapa de procesado de transporte para finalmente abordar la subcapa de control de transporte.

1) Subcapa de procesado de transporte

La Figura 3 muestra dos elementos que conforman las entidades funcionales en la parte de la subcapa de procesado de transporte de la red de acceso: el PCEF y el BBERF, las cuales vamos a definir a continuación.

a) Función de Aplicación de Políticas y Cargos Asociados (PCEF): Esta entidad funcional, que en inglés se traduce cómo *Policy and Charging Enforcement Function,* está localizada en el PDN GW y se encarga de aplicar las políticas de QoS que definen las reglas PCC que uno o más PCRFs le indiquen a través de punto de referencia Gx. Esto significa que esta entidad funcional clasifica los flujos IP y aplica las políticas de QoS asociadas a cada SDF activada (definidas en cada regla PCC) para cada usuario tanto en subida (*uplink* o sentido UE-PDN) como en bajada (*downlink* o sentido PDN-UE). La PCEF implementa los túneles EPS en uno de sus extremos, mapeando en bajada (*downlink*) todos los flujos de cada SDF en el túnel que mejor garantice la QoS en el camino que recorren hasta el UE.

PCRF

Responde a las siglas en inglés de *Policy and Charging Rules Function* y es el elemento de la subcapa de control de transporte del PCC que toma las decisiones en cuanto a control de admisión sobre las solicitudes de recursos.

Así pues, el PCEF es un único elemento que aglutina un gran número de funciones en la aplicación de políticas (control de acceso, NAT/NAPT, asignación de tráfico IP a túneles EPS, etc.) incluyendo funciones que afectan al reporte de eventos hacia el PCRF para notificar la modificación o el establecimiento de un túnel EPS por parte del usuario (modo *pull* de solicitud de recursos) o también incluyendo funciones relacionadas directamente a la facturación del servicio en uso.

Por ejemplo, el PCEF debe asegurarse de que, si un paquete IP ha sido descartado como resultado de la aplicación de una política o debido al cargo asociado a un flujo, nunca deberá ser reportado para facturación *offline* ni será causa de consumo de crédito en la facturación *online*.

Las **reglas PCC** son en realidad el resultado de las decisiones a nivel de sesión que la entidad funcional PCRF (servidor de políticas en la subcapa de control de transporte) toma una vez ha evaluado información de disponibilidad de recursos de la red y políticas del operador de la misma red. Es una decisión de control de admisión a nivel de SDFs (cuya descripción, por ejemplo, puede ser recibida desde el punto de referencia Rx) y las reglas PCC son el resultado de ésta.

OCS y OFCS

Responden a las siglas en inglés de *Online Charging System* y *Offline Charging System*.

Interfaz Gy

La interfaz entre PCEF y OCS es el Gy. Utilizada para transferir información de facturación *online* (prepago). El 3GPP recomienda el protocolo Diameter para su implementación (TS 32.299).

Así pues, los SDFs (asociados a cada regla PCC a modo de entradas de clasificación de tráfico) también pueden estar sujetos a un control de facturación si el servicio al que van asociados así lo requiere. Consecuentemente, el PCEF debe estar al corriente de dicho control también. De hecho, el 3GPP ha definido dos interfaces dedicadas con las entidades funcionales de facturación OCS y OFCS con unos puntos de referencia llamados Gy y Gz respectivamente.

Por ejemplo, para el caso de tener un SDF sujeto solo a control de facturación, el PCEF permite que un SDF (definido por una regla PCC activa) que esté sujeto a control de facturación pase a través de él si y sólo si existe una regla PCC activa asociada y la entidad OCS ha autorizado el crédito para el uso del servicio.

Para el caso de tener un SDF que esté sujeto a ambos controles de políticas de QoS y de facturación, PCEF solamente permite el paso de dicho flujo de datos a través de él si y sólo si se dan las condiciones de control de políticas y facturación correctas. Es decir, que el correspondiente acceso (a nivel de cortafuegos) haya sido habilitado y, en el caso de facturación *online*, el OCS haya autorizado el crédito para el servicio asociado a los flujos.

Finalmente, para el caso de que un flujo de datos de servicio esté sujeto solo a control de políticas y no a control de facturación, el PCEF permite el paso de dicho flujo de datos a través de él si y sólo si se cumplen las condiciones impuestas por las políticas correspondientes.

b) Función de Asociación de Túneles y Reporte de Eventos (BBERF): Esta entidad funcional, que en inglés se llama *Bearer Binding and Event Reporting Function,* está mapeada sobre el SGW en la arquitectura EPS y está interconectada con el PCRF vía el punto de referencia Gxx.

Tal y como las siglas indican, este elemento es capaz de mapear el tráfico a los túneles EPS. Puede surgir la pregunta de para qué el BBREF realiza esta función si el PCEF ya lo hace como extremo del túnel. Esto es debido a que dependiendo del tipo de protocolo de movilidad usado en el EPC la función de asignación de túneles se realiza en el PCEF (protocolo GTP) o en el BBERF (protocolo IP mobile).

La capacidad de reporte de eventos al PCRF también puede estar asociada a esta entidad funcional con las mismas condiciones mencionadas con respecto al PCEF. Con lo cual es posible que en una red de acceso móvil no exista el BBERF ni la interfaz Gxx.

2) Subcapa de control de transporte

En el modelo del 3GPP, esta subcapa está formada por dos entidades funcionales: SPR y PCRF. Aquí hemos incluido también las dos entidades extras encargadas del control de cargos asociados: el OCS y el OFCS que ya han sido mencionadas anteriormente.

a) Repositorio de Perfiles de Suscripción (SPR): Esta entidad funcional llamada en inglés *Subscriber Profile Repository* almacena los perfiles de usuario a nivel de capa de transporte (entre otros parámetros el GBR y el MBR asociados a dicho usuario y lista de servicios permitidos) y está interconectado con el PCRF a través de una interfaz llamada Sp. Se transfiere dicha información de perfil al PCRF para que la tenga en cuenta a la hora de realizar el control de

Interfaz Gz

La interfaz entre PCEF y OFCS es el Gz. Utilizada para transferir información de facturación *offline* (pospago). El 3GPP recomienda el protocolo Diameter para su implementación (TS 32.299).

GTP

Los operadores de red móvil usan el *GPRS tunneling protocol* (GTP) en varias interfaces en itinerancia, red de acceso de radio y dentro de la red troncal en redes 3G y 4G para llevar el servicio general de radio por paquetes (GPRS). GTP permite a los suscriptores móviles usar sus teléfonos (UE) para mantener una conexión a una Packet Data Network (PDN) para el acceso a Internet mientras están en movimiento.

Interfaz Sp

La interfaz entre PCRF y SPR es el Sp. Utilizada por el PCRF para obtener del SPR información de suscripción a nivel de red de acceso LTE. El 3GPP recomienda el protocolo Diameter para su implementación (TS 23.203).

GBR y MBR

Responden a las siglas en inglés de *Guaranteed Bit Rate* y *Maximum Bit Rate*.

admisión y generar las correspondientes reglas PCC. Este elemento está normalmente integrado en la misma plataforma que el HSS (*Home Subscriber Server*) aunque puede ser una entidad funcional por separado.

b) Función de Reglas de Políticas y Facturación (PCRF): En inglés responde a las siglas de *Policy and Charging Rules Function* y es el elemento que toma las decisiones en cuanto a control de admisión sobre las solicitudes de recursos recibidos desde el AF (*Application Function*) a través del punto de referencia Rx (modo *push*) o desde el PCEF vía la interfaz Gx/Gxx (modo *pull*). También controla las tareas del PCEF con respecto al control de facturación (y su interacción con el OCS y el OFCS).

Para el 3GPP, el **AF (*Application Function*)** es la entidad de la subcapa de control de servicio que es capaz de extraer la información de descripción de sesión de servicio con la petición de recursos y remitirla con el formato adecuado al PCRF vía la interfaz Rx. El 3GPP contempla que si el servicio está basado en IMS el AF está implementado en el P-CSCF y si no está basado en IMS entonces es una entidad equivalente. Lo importante es que la solicitud de recursos de la sesión de servicio cumpla con la especificación de la interfaz Rx definido por el 3GPP.

Desglosando paso a paso las tareas que realiza el PCRF con un poco más de detalle, se obtiene la siguiente lista en este orden:

1) **Autorización de la solicitud de recursos de servicio y control de admisión de suscripción:** En el caso de recibir una solicitud de recursos de servicio vía la interfaz Rx, el PCRF comprueba que dicha descripción de la sesión de servicio es acorde con las políticas del operador (políticas arbitrarias). Si supera este filtro comprueba que dicha solicitud es acorde con la información de suscripción (almacenada en el SPR) del usuario que la ha solicitado. En caso de que no se cumpla sólo una de estas dos comprobaciones la sesión se rechaza. Es en definitiva lo que se llama el control de admisión.

2) **Autorización de la QoS (generación de reglas PCC):** El PCRF usa la información de descripción de servicio recibida desde el AF y/o la información de suscripción para extraer la autorización de QoS para los SDFs extraídos de dicha descripción. Los parámetros de autorización de QoS son principalmente el QCI y los GBR y MBR correspondientes, si aplican. El PCRF puede tener en cuenta también las solicitudes de QoS recibidas desde el PCEF vía la interfaz Gx.

3) **Reporte de eventos:** El PCRF puede por ejemplo reportar eventos ocurridos en la capa de transporte (estatus de túneles EPS o sesiones EPS) o even-

HSS

En inglés responde a las siglas de *Home Subscriber Server*. Base de datos que almacena la información de suscripción de un usuario junto con información de autenticación y autorización a nivel de servicio (explicado en la sección 3 donde se describe el modelo de referencia del 3GPP para la capa de servicio).

P-CSCF

Proxy Call Session Control Function.

Componente del núcleo IMS que ejerce de elemento fronterizo con el equipo de usuario a nivel de señalización SIP (IMS). Es una entidad funcional definida por el 3GPP y que se explica en la sección 3.

Interfaz Rx

La especificación por parte de la 3GPP de dicho interfaz está descrita en el documento TS 29.214.

QCI

Responde a las siglas de *QoS Class Identifier* y define el grupo de características a nivel de calidad de servicio de un tipo de tráfico. Es un término básico utilizado en redes LTE y clave para la garantía de la calidad de servicio. Se describe con más detalle más adelante.

tos de facturación al AF si éste lo ha solicitado expresamente vía la interfaz Rx.

El PCRF soporta la comunicación con otros PCRFs de dominios administrativos distintos para el escenario de itinerancia. Dicha comunicación se realiza a través de un punto de referencia dedicado llamado S9. En este caso, se derivan dos instancias del PCRF según en qué dominio administrativo se encuentra: el V-PCRF para el control de la red visitada y el H-PCRF para el control de la red donde el usuario móvil pertenece como suscriptor.

Interfaz S9

La interfaz entre el PCRF y otro PCRF de un dominio administrativo distinto (otro operador) es el S9. Utilizada por el PCRF para solicitar recursos en una red LTE distinta a la suya y cuando un suscriptor de su red se encuentra en ella (itinerancia). El 3GPP recomienda el protocolo Diameter para su implementación (TS 29.215).

c) Sistema de Facturación *Online* (OCS): El *Online Charging System* realiza la gestión del crédito para la facturación de prepago. Dentro de esta entidad funcional reside la funcionalidad de control de crédito basado en los flujos de datos de servicio que realiza el control del crédito *online*. El PCEF interactúa con esta entidad para comprobar el crédito y reporta el estatus de este sobre el punto de referencia Gy.

Un ejemplo de este tipo de facturación es cuando tenemos un límite en el volumen de datos a gastar en un mes. Si se supera tal límite, la velocidad máxima de descarga baja.

Arquitectura PCC

Llama la atención cómo el modelo de arquitectura PCC define con dos bloques específicos las tareas de facturación, así como su interacción con elementos de procesado de transporte. Es un aspecto que el 3GPP quiere dejar bien especificado debido al gran consumo que la telefonía móvil ha conseguido.

d) Sistema de Facturación *Offline* (OFCS): El *Offline Charging System* se encarga de aglutinar los eventos de facturación recibidos desde el PCEF vía un punto de referencia llamado Gz para generar registros de facturación. Estos registros (Charging Data Records) se envían luego al sistema de generación de facturas.

De estos registros sale posteriormente la factura que nos llega a casa por correo o por e-mail.

Los *EPS Bearers* y los QCIs

Túnel EPS

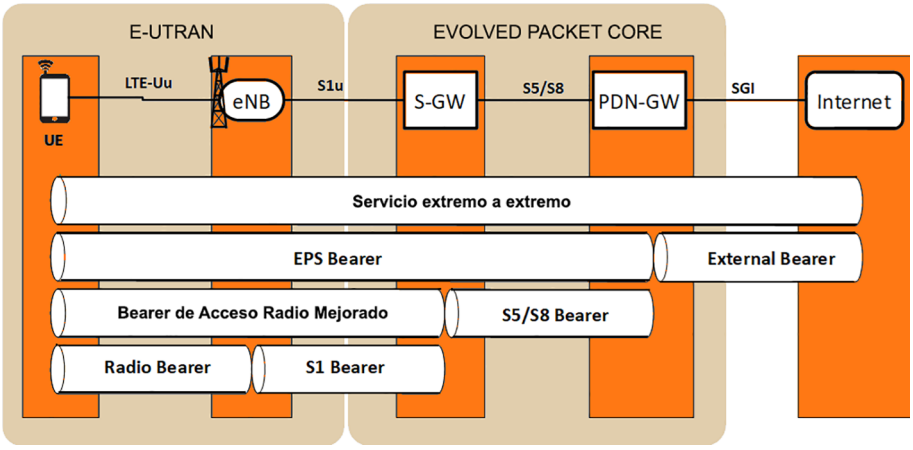
Como ya hemos comentado anteriormente, el 3GPP ha definido un concepto más abstracto asociado al túnel EPS en los documentos de especificación como IP-CAN bearer o *IP-Connectivity Access Network bearer*. Hay dos tipos de IP-CAN o EPS *bearer*: *default bearer* y *dedicated bearer*.

Para empezar, vamos a definir con más detalle el concepto de ***IP-CAN bearer*** o también llamado ***EPS bearer***. El *EPS bearer* es un canal virtual con unas características de QoS y ancho de banda particulares. Es decir, es una especie de túnel cuyos extremos van desde el propio equipo de usuario (UE) hasta la PDN GW y todo paquete IP que entre en dicho túnel gozará de un tratamiento a nivel de garantía de QoS específica a lo largo de todo el EPC.

Túnel EPS. Cuando un paquete IP llega al eNodeB, éste mapea el túnel EPS a una portadora radio de características similares de QoS. Es muy importante entender que el mapeo que el eNodeB realiza entre un túnel EPS y una portadora radio es de uno a uno. El estándar del 3GPP prohíbe explícitamente que más de un túnel EPS se pueda mapear a una sola portadora radio.

Un *EPS bearer* es en realidad la agrupación de varios *bearers* establecidos entre los elementos del EPC y de E-UTRAN. En la Figura 4 se puede ver cómo se divide un *EPS bearer*.

Figura 4. EPS bearers y su desglose entre entidades del EPC.



Así, un solo equipo de usuario (UE) puede tener más de un *EPS bearer* establecido con la correspondiente PDN GW y cada uno tiene sus propias características de QoS. Los túneles EPS pueden ser unidireccionales o bidireccionales y pueden ser establecidos, modificados o liberados por el propio UE o por la red de acceso (MME o PCRF). Existen dos tipos de *bearers*:

Número máximo de EPS bearers

El número máximo de *EPS bearers* simultáneos que un UE puede soportar es de 11.

- **Default**: es un túnel EPS que se establece de manera automática por la red de acceso cuando el equipo de usuario se adhiere a la red de acceso LTE (MME) y se le asigna una dirección IP (activación de una sesión EPS). A este tipo de *bearer* se le asigna siempre un QCI de tipo Non-GBR (ver Tabla 1). Este túnel se mantiene hasta que el terminal se apaga.

- **Dedicado**: son túneles que se establecen bajo petición expresa del PCRF o del equipo de usuario cuando se invoca un servicio que requiere de una QoS distinta a la ofrecida por el *default bearer* (por ejemplo, una llamada de voz). Este tipo de túneles pueden tener asignados cualquier QCI: de tipo GBR o Non-GBR. Solo son establecidos si previamente el *default bearer* ya existe.

Un UE puede tener asignados varios túneles EPS simultáneos tanto *default* (porque está asociado a más de un APN) como dedicados con diferentes características de QoS.

¿Qué parámetros define el 3GPP para caracterizar a nivel de QoS un túnel EPS y donde se aplican dichos parámetros a lo largo del EPS?

El 3GPP ha definido cuatro parámetros, los cuales ya se han ido mencionando anteriormente:

1) ***QoS Class Identifier*** **(QCI):** que define el comportamiento de QoS del tráfico asociado a un túnel EPS. Este parámetro, existente en la cabecera del túnel, es consultado en todos los nodos del EPC y E-UTRAN ya que es un parámetro muy importante en el mapeo de cada *bearer* entre dichos nodos (ver la Figura 4).

Un **QCI o *QoS Class Identifier***, identifica los valores de un conjunto de parámetros que definen cómo se va a tratar el tráfico a lo largo de los nodos que conforman el EPS. Estos parámetros son cuatro en total:

- **Tipo de recurso** (con dos valores posibles: GBR velocidad de bit garantizada o Non-GBR velocidad de bit no garantizada),
- **Prioridad** (valor entero del 1 al 9, que indica el nivel de prioridad respecto a otros flujos),
- **Retardo de paquete** (el retardo máximo deseado para un paquete IP entre el UE y la PDN GW)
- **Tasa de pérdida de paquetes** (la tasa de pérdida de paquete máxima deseada entre el UE y la PDN GW).

El 3GPP ha estandarizado un mínimo de 9 QCI, con valores asignados a los respectivos parámetros, para 9 tipos de servicios predefinidos. Estos valores pueden verse en la Tabla 1.

QCIs

A pesar de que los 9 valores de QCI son los que se implementan en redes LTE, el 3GPP sigue ampliando la lista de QCIs en los sucesivos *releases* de sus especificaciones para cubrir otros servicios como por ejemplo los de tipo *critical mission*. El documento del 3GPP donde se define la lista más actualizada es el TS 23.203 "*Policy and Charging Control*".

Tabla 1. Lista de QCI.

QCI	Tipo de bearer	Prioridad	Retardo de paquetes	Pérdida de paquetes	Ejemplo de aplicación
1	GBR	2	100 ms	10^{-2}	Llamada VoIP (voz)
2		4	150 ms	10^{-3}	Llamada de videoconferencia (vídeo)
2		3	50 ms		Juegos en línea (tiempo real)
4		5	300 ms	10^{-6}	Transmisión de video
5	Non-GBR	1	100 ms		Señalización IMS
6		6	300 ms		Vídeo (Flujo de Transmisión) Basado en TCP (por ejemplo, www, correo electrónico, chat, ftp, p2p, o similares)
7		7	100 ms	10^{-3}	Voz, Vídeo (Transmisión en directo), Juegos interactivos
8		8	300 ms	10^{-6}	Vídeo (Flujo de Transmisión) Basado en TCP (por ejemplo, www, correo electrónico, chat, ftp, p2p, o similares)
9		9			Vídeo (Flujo de Transmisión) Basado en TCP (por ejemplo, www, correo electrónico, chat, ftp, p2p, o similares). Tipicamente utilizado como bearer por defecto

2) *Allocation and Retention Priority* (ARP): este parámetro indica cuán importante (nivel de prioridad) es el túnel EPS con respecto a otros túneles. La consulta de este parámetro se aplica principalmente en nodos del EPC donde se realiza conformación de tráfico como el eNodeB y el PDN-GW.

Pongamos un ejemplo: ¿Qué sucede si en un momento determinado un usuario se mueve a una celda que está muy congestionada y la migración de sus túneles EPS no se puede realizar porque no hay recursos suficientes? Pues hay que desalojar otros túneles EPS activos y el parámetro ARP es el que nos dirá cuáles son los menos importantes y, por lo tanto, los candidatos a ser liberados.

3) *Guaranteed Bit Rate* (GBR): indica la cantidad garantizada de bits por segundo que se necesitan (capacidad reservada) para este túnel EPS. Este parámetro solo se especifica cuando el túnel EPS tiene un QCI asignado de tipo GBR. El parámetro GBR puede modificarse si se requiere una ampliación o dis-

minución del volumen de tráfico a garantizar. La garantía del *bit rate* se aplica principalmente en el eNodeB y en el PDN-GW tanto para el tráfico de subida (*uplink*) como de bajada (*downlink*).

Pongamos un ejemplo: ¿Qué sucede si ya existe un SDF (regla PCC) que utiliza un túnel con un QCI en concreto y de repente aparece un SDF o regla PCC nueva que requiere de un túnel con el mismo QCI? No se establecerán dos túneles con el mismo QCI si no que se modificará el ya existente ampliando el GBR asociado para hacer sitio al nuevo flujo de la segunda regla PCC.

4) *Maximum Bit Rate* (MBR): indica la cantidad máxima de bits por segundo permitida (de pico) para este túnel EPS. Este parámetro solo se especifica cuando el túnel EPS tiene un QCI asignado de tipo GBR. En tráfico de subida (*uplink*) esta conformación de tráfico se produce en el propio UE y posteriormente en el eNodeB. En tráfico de bajada (*downlink*) esta conformación de tráfico se produce en el PDN-GW.

Maximum Bit Rate

Cabe destacar que el parámetro de *Maximum Bit Rate* (MBR) sí que se especifica para un SDF de tipo Non-GBR mientras que en el caso de un túnel EPS no se especifica (en su lugar aplica el UE-AMBR y APN-AMBR).

A parte de los cuatro parámetros de QoS que se asocia a cada *EPS bearer* mencionados anteriormente, hay otros dos parámetros QoS que se asocian al perfil de usuario a nivel de red de acceso LTE y que también se tienen en cuenta en la conformación del tráfico:

1) *APN-Aggregated Maximum Bit Rate* (APN-AMBR): indica la cantidad máxima de bits por segundo permitida (de pico) en subida y bajada (*uplink* y *downlink*) para el agregado de todos los túneles EPS de tipo Non-GBR asociados a un APN (entre el UE y una PDN-GW en concreto). Es decir, que si un UE está asociado a dos APNs se aplicarán dos parámetros como este por separado, uno por cada APN. Esta conformación de tráfico en bajada (*downlink*) se aplica exclusivamente en el PDN-GW. En subida (*uplink*), se aplica en dos lugares: el mismo UE antes de encapsular y mapear el tráfico saliente en los túneles EPS y de nuevo en el PDN-GW antes de enviar los paquetes fuera del EPS.

2) *UE-Aggregated Maximum Bit Rate* (UE-AMBR): indica la cantidad máxima de bits por segundo permitida (de pico) en subida y bajada (*uplink* y *downlink*) para el agregado de todos los túneles EPS de tipo Non-GBR asociados a un UE. Este límite se aplica a todo el tráfico Non-GBR de un usuario independientemente de si está asociado a más de un APN o no. Esta conformación de tráfico la aplica el eNB tanto en subida (*uplink*) como en bajada (*downlink*) cuando realiza el mapeo de los *radio bearers*.

Los *Service Data Flows* y su mapeo a los *EPS bearers*

Ya hemos mencionado los **flujos de datos de servicio (*Service Data Flows*)** cuando hemos descrito la regla PCC. Se definen una serie de filtros de flujos IP que ayudarán al PCEF (PDN GW) a mapear los diferentes flujos IP a cada servicio y además a aplicar los parámetros QoS asociados a cada servicio activado vía la regla PCC correspondiente.

Los **flujos de datos de servicio** (o ***Service Data Flows***) se definen como un agregado de flujos de paquetes IP cada uno de ellos caracterizados por la tupla de 5 parámetros típica: direcciones IP tanto de origen como de destino, puertos usados en origen y destino y el protocolo. Igual que con los túneles EPS, cada SDF especificado por el PCRF se clasifica en dos tipos: GBR y Non-GBR.

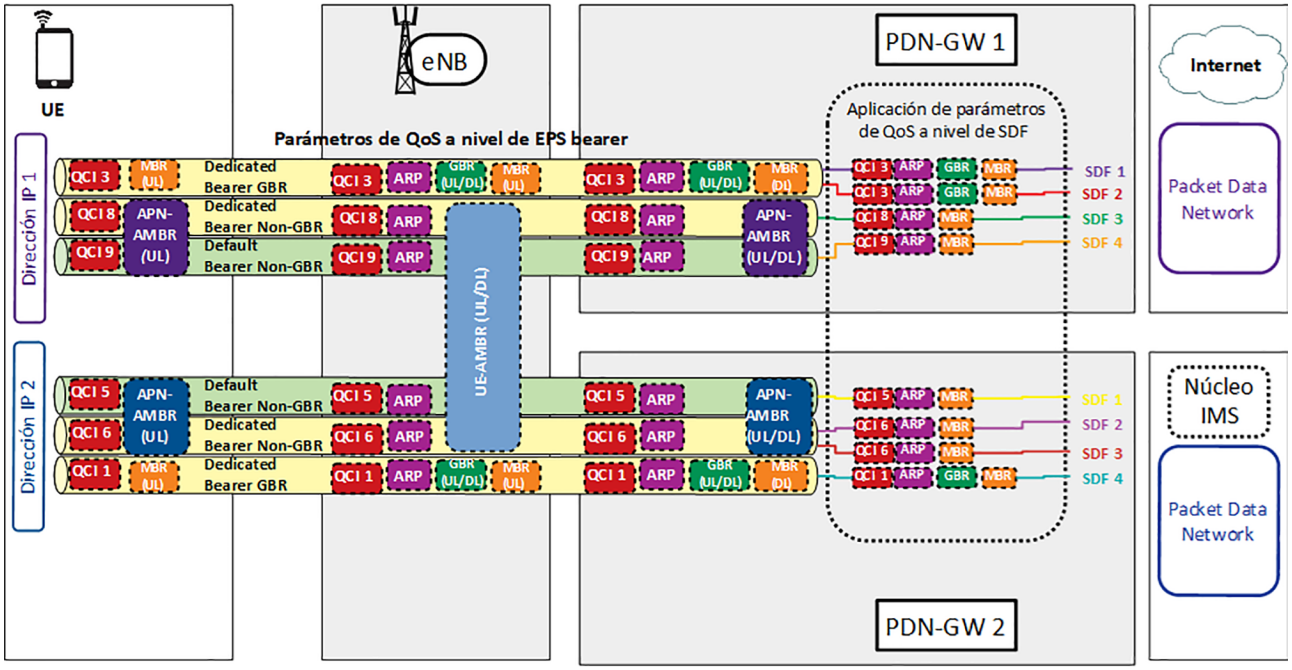
A cada uno de estos SDFs se les asocian unos parámetros de QoS particulares los cuales son independientes a los fijados a cada túnel EPS.

Para un SDF de tipo GBR los parámetros de QoS especificados son: QCI, ARP, GBR (*uplink*/*downlink*), MBR (*uplink*/*downlink*).

Para un SDF de tipo Non-GBR los parámetros de QoS especificados son: QCI, ARP, MBR (*uplink*/*downlink*).

Los parámetros de QoS a nivel de SDF y a nivel de túnel EPS se aplican de manera independiente. Mientras los primeros se aplican exclusivamente en el PDN-GW (tanto para tráfico de subida como de bajada) la aplicación de los segundos se distribuye a lo largo de todo el EPS como ya hemos explicado anteriormente y tal y como se puede ver en la Figura 5.

Figura 5. Aplicación de parámetros QoS en EPS bearers y SDF a lo largo del EPC.



El mapeo entre un tráfico IP que ya ha sido asignado a un SDF y un túnel EPS se realiza principalmente mediante una correspondencia directa entre el QCI del perfil QoS del SDF y el QCI del túnel EPS. Esta correspondencia se realiza

realmente aplicando otros filtros IP específicamente pensados para clasificar el tráfico IP dentro de los túneles EPS. Dichos filtros se llaman *Traffic Filtering Templates* (TFT).

En el sentido de bajada (*downlink*), este mapeo SDF túnel EPS parece evidente ya que la clasificación previa a SDF se produce en el PDN GW, pero ¿qué sucede en el sentido opuesto (*uplink*)?

En subida el UE aplica directamente los TFT (proporcionados al UE durante el establecimiento o actualización del túnel EPS) para clasificar el tráfico IP de las aplicaciones al túnel EPS correspondiente. Como ya hemos dicho, el tráfico se clasifica a nivel de SDF en el PDN-GW tanto en subida como en bajada para aplicar sus propios parámetros QoS.

2.3. Elementos del *mobile offload*

Volviendo a la Figura 2 mostrada al principio, aparecen las redes Wi-Fi como una red de acceso que el UE puede usar para acceder a los servicios contratados con el operador de red. Esta red de acceso se considera como *non-3GPP* ya que no ha sido especificada por este organismo. No obstante, dichas redes están prácticamente en cualquier espacio público (bibliotecas, recintos deportivos, centros comerciales, etc.) y también en recintos privados (hoteles, casas particulares, empresas, etc.) y se han acabado integrando en el contexto de especificación de este organismo.

¿Cómo detecta un UE si está en una red Wi-Fi confiable o no confiable?

Hay varias maneras. Podría ser que el UE tuviera preconfiguradas una serie de políticas estáticas o que el propio operador comunique al UE si es una Wi-Fi confiable o no usando un protocolo que debe ser soportado por el UE (llamado AN-DSF) o finalmente que se aproveche la propia señalización de autenticación (EAP-AKA) en el punto de acceso para transferir esta información al UE.

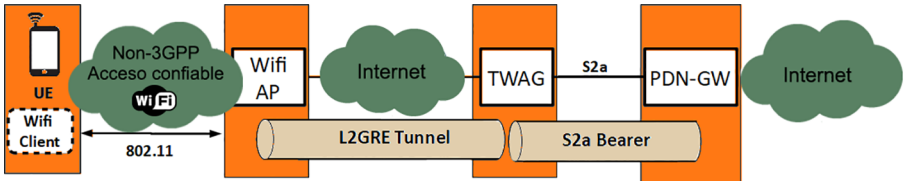
En la mencionada figura aparecen dos pasarelas según si la red Wi-Fi desde la que se conecta es confiable (*trusted*) o no confiable (*untrusted*) desde el punto de vista del operador de telefonía móvil.

Una **red Wi-Fi confiable** es aquella que está gestionada por el propio operador y a la cual solo pueden asociarse suscriptores de dicho operador.

Un ejemplo de estas redes son las existentes en las tiendas de los propios operadores.

La autenticación en estas redes se realiza vía las credenciales de la propia USIM del equipo de usuario. Entre el UE y el punto de acceso de Wi-Fi no hay más que una conexión Wi-Fi normal y desde el punto de acceso al punto de anclaje de la red del operador se establece un túnel sin encriptación. Este punto de anclaje se llama **TWAG** o ***Trusted WLAN Access Gateway***.

Figura 6. Integración del EPC con redes Wi-Fi confiables.



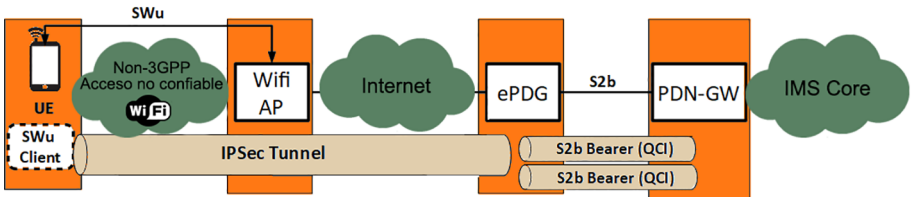
La particularidad de usar esta red Wi-Fi es que se concibió (hasta el *release* 11 de la especificación del 3GPP) para que el UE descargara la red de acceso LTE del tráfico a Internet. Es decir que la PDN-GW a la que se conecta el TWAG es exclusivamente la correspondiente al APN de Internet. Y de hecho el TWAG especificado en este *release* solo permite la asignación de una dirección IP y conectividad a un PDN-GW por defecto, el del APN de Internet.

Conexión multi APN con TWAG

En el *release* 12 de la especificación del 3GPP se ha incluido una modificación en la arquitectura para que el nuevo TWAG permita que desde una red confiable un UE pueda acceder a más de un APN posibilitando llamadas IMS por Wi-Fi. Esto conlleva que el UE deba soportar ciertas capacidades a nivel de firmware que con el *release* 11 no hacía falta.

Una **red Wi-Fi no confiable** es aquella que no ha sido desplegada por el propio operador, que es el caso más típico hoy en día. En este caso el UE tiene que establecer un túnel IPSec (interfaz llamada SWu en la especificación 3GPP) con el punto de anclaje, la cual es una pasarela dedicada. Dicha pasarela es la **ePDG o *Evolved Packet Data Gateway*** y está pensada para proporcionar conectividad con la PDN-GW que da acceso al núcleo IMS y así poder realizar llamadas de voz usando el propio *dialpad* de marcado del terminal sin necesidad de instalar ninguna aplicación extra.

Figura 7. Integración del EPC con redes Wi-Fi no confiables.



Núcleo IMS

IMS responde a las siglas de *IP Multimedia Subsystem*. Como veremos en la sección 3, es el modelo de referencia para el procesado de la señalización de establecimiento y liberación de sesiones multimedia.

Como se puede ver en la Figura 7, entre el ePDG y el PDN-GW se establecen *bearers* o túneles dedicados con sus respectivos QCIs (interfaz S2b), los cuales pueden ser por ejemplo para la señalización IMS (QCI 5) y para el tráfico de voz (QCI 1) según las sesiones que va estableciendo el usuario.

Wi-Fi Calling

El primer operador en España en ofrecer *Wi-Fi calling* a sus suscriptores ha sido Orange, aunque sin *handover* transparente con la red móvil.

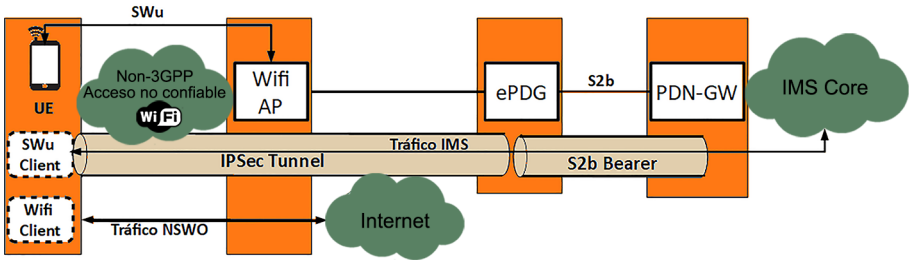
***Wi-Fi calling*, llamadas Wi-Fi** o **VoWiFi** son los nombres comerciales usados para denominar dicho servicio de llamadas IMS por Wi-Fi. A diferencia del caso de la Wi-Fi confiable, en el caso del acceso a una Wi-Fi no confiable, el usuario debe tener un terminal móvil que soporte esta tecnología, a parte también de que el propio operador haya implementado este tipo de conexión.

A pesar de utilizar el núcleo IMS y el protocolo SIP para la señalización de establecimiento de llamada como en VoLTE, **la QoS no está garantizada extremo a extremo** ya que el tráfico atraviesa la red Wi-Fi, la cual no está gestionada por el propio operador. Así que se asume que hay sobredimensionamiento de la capacidad de la red de acceso entre el UE y el ePDG que en la mayoría de los casos no debería sufrir colapsos ante una llamada de voz.

En un escenario de Wi-Fi no confiable, ¿cómo encamina el UE el tráfico que no es de servicios IMS, como por ejemplo Internet?

Uno podría pensar que puede utilizar el mismo cliente SWu que incorpora el terminal y establecer más *bearers* en la interfaz S2b, pero al estar conectado al APN de IMS esta conexión se realiza de otra manera gracias a la definición por parte del 3GPP del NSWO (*Non-Seamless WLAN Offload*). Es una prestación que debe soportar también el propio terminal en el cual le indica que para llamadas IMS use la interfaz SWu (túnel IPSec) pero para tráfico no-IMS use directamente la Wi-Fi de manera transparente (ver Figura 8).

Figura 8. NSWO en redes Wi-Fi no confiables.



WebRTC

WebRTC responde a las siglas en inglés de ***Web Real-Time Communications*** y es el nombre de un entorno o estándar que extiende las capacidades del navegador de web. Este estándar ha sido definido por el W3C partiendo de un proyecto en código abierto que es apoyado por grandes compañías tecnológicas como Google, Mozilla Foundation, Opera *Software* y Apple. Posibilita comunicaciones multimedia *peer-to-peer* utilizando el propio navegador web y está compuesto por tres componentes principales: audio, video y datos.

W3C

Responde a las siglas de *World Wide Web Consortium*. Con sede en el MIT (*Massachusetts Institute of Technology*), tiene como objetivo desarrollar protocolos y directrices que garantizan el crecimiento a largo plazo de la Web. (http://www.w3.org)

Básicamente encapsula en sendos *web-socket* la información de audio y video capturados del micrófono y la cámara del terminal (PC o smartphone) directamente desde el navegador.

Web-socket

Es una tecnología que proporciona un canal de comunicación bidireccional y *full-duplex* sobre un único socket TCP. Está diseñada para ser implementada en navegadores y servidores web, pero puede utilizarse por cualquier aplicación cliente/servidor. El IETF ha definido sus características en el RFC 6455.

Las últimas versiones de prácticamente cualquier navegador existente ya soportan WebRTC (principalmente debe soportar HTML5).

> Ello permite integrar en la propia web comunicaciones multimedia que están teniendo mucho éxito en páginas donde se requiera algún tipo de interacción con algún servicio de atención al cliente o asesoramiento, como por ejemplo webs de bancos o incluso atención médica remota.

La principal ventaja de usar WebRTC es la integración total de comunicaciones multimedia en el propio navegador convirtiéndolo en un terminal de comunicaciones y enriqueciendo la experiencia del usuario.

La principal desventaja es que, no hay garantía de QoS en dicho intercambio multimedia. Se asume que la conectividad a Internet es suficientemente holgada como para garantizar una mínima calidad.

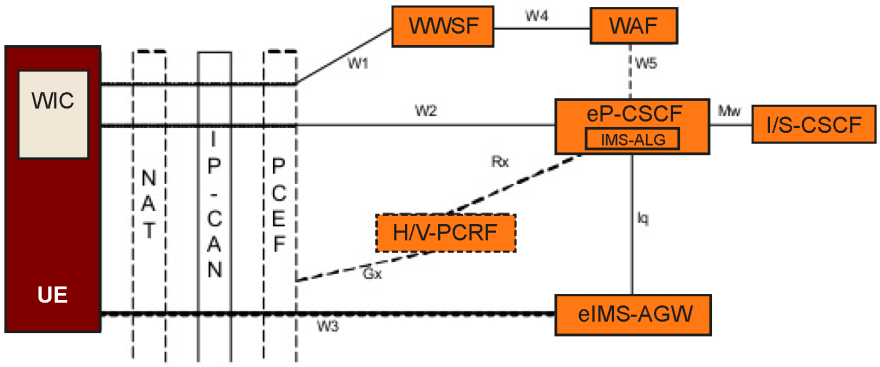
La especificación de este estándar solo define cómo negociar los componentes multimedia (códecs de voz y video, por ejemplo) entre dos navegadores web (usando el protocolo SDP) pero no especifica ningún mecanismo de establecimiento de llamada. Éste último se tiene que realizar mediante otros mecanismos y protocolos que este estándar no abarca.

Protocolo SDP

Session Description Protocol. Protocolo para negociar parámetros multimedia de establecimiento de sesión (códecs o puertos UDP donde enviar los flujos RTP). Está especificado en el RFC4566.

La señalización SIP que el estándar IMS incluye puede ser una manera de permitir que esta información de negociación pueda ser intercambiada y así añadir otro tipo de UE desde el cual poder acceder a los servicios contratados. No obstante, la integración de IMS con WebRTC no es trivial. El 3GPP ha realizado esfuerzos para proponer una especificación sobre cómo integrarlo (TS 24.371) y básicamente propone lo siguiente:

Figura 9. Modelo de referencia propuesto por el 3GPP para integrar WebRTC e IMS.



P-CSCF

El P-CSCF es un elemento que pertenece a la capa de servicio, en concreto al núcleo IMS. Dicho elemento está descrito en detalle en la sección 3.1.3.

- Un **WIC (*WebRTC IMS Client*)** sería integrado en el propio código de la web (javascript) para implementar un *stack* sencillo que proporcione el cliente IMS en el propio navegador. Toda la señalización entre el UE y el eP-CSCF seria encapsulada en un *web-socket* específico para la señalización IMS.

- Un **eP-CSCF (*enhanced P-CSCF for WebRTC*)** que se encargaría de realizar las funciones del P-CSCF con la particularidad de el encapsulamiento y desencapsulamiento en *web sockets* de toda la señalización IMS intercambiada con el UE (interfaz W2).

- Un **WWSF (*WebRTC Web Server Function*)** que sería el servidor web donde se alberga la página en la que está integrado el WIC. El usuario deberá conectarse a este servidor (interfaz W1) como primer paso y así descargarse dicha web. Este elemento puede estar en un servidor separado (proporcionado por un tercero) o integrado en el propio eP-CSCF. Esta entidad incluye un **WAF (*WebRTC Authorization Function*)** que se encarga de autenticar al usuario (interfaz W4) con sus credenciales cuando este intenta descargarse la web.

- Un **eIMS-AGW (*enhanced IMS Access Gateway for WebRTC*)** que realizaría las funciones de pasarela multimedia para los flujos de voz, video y datos que llegan encapsulados en los respectivos *web-sockets* (interfaz W3).

El conjunto del eP-CSCF más el eIMS-AGW harían las funciones del WebRTC GW que aparece en la Figura 2 expuesta al principio.

3. Capa de servicio

En la capa de servicio hay un subconjunto de elementos dentro de la misma que es predominante como plataforma de provisión y habilitación de servicios multimedia y que queremos destacar: el **núcleo IMS**. El 3GPP, como creadora del IMS, centra su arquitectura de control de servicio en esta tecnología y es lo que se describirá en detalle en las siguientes secciones.

El **núcleo IMS** se encarga de recibir y procesar la señalización de establecimiento de sesiones de servicio multimedia (SIP) proveniente de los usuarios y además cumple con las siguientes funciones:

- Almacenamiento de perfiles de usuario a nivel de servicio.
- Mecanismos asociados de registro, autenticación y autorización.
- Negociación de prestaciones (como los codificadores de voz y vídeo en el establecimiento de una videoconferencia) y control de recursos (con las subcapas de transporte).
- Encaminamiento de señalización hacia destinatario basado en direcciones de dominio.

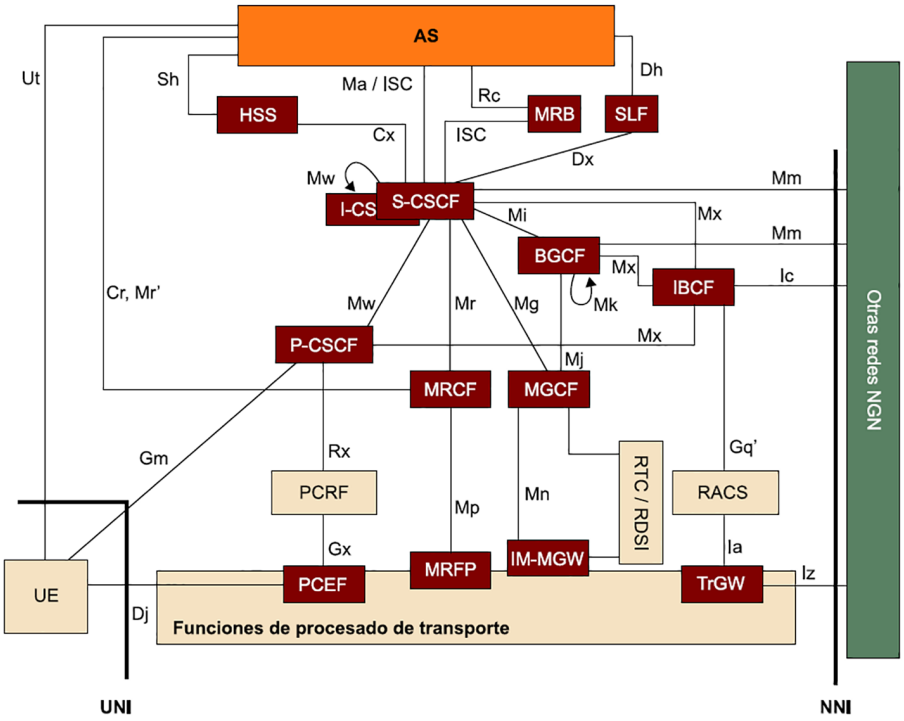
Normalmente el núcleo IMS sirve a un solo dominio administrativo y éste está asociado a un operador, del cual los usuarios son suscriptores de una lista de servicios, representados por los AS (*Application Servers* y que veremos en la sección 4) a los que acceden a través del núcleo IMS.

A continuación, vamos a ver una descripción detallada de las entidades que conforman un núcleo IMS y cómo interactúan entre ellas según el servicio que se invoca desde el usuario.

3.1. Componentes del núcleo IMS

En la Figura 10 se puede ver la arquitectura de referencia que el 3GPP define para el núcleo IMS.

Figura 10. Arquitectura de referencia de IMS para 3GPP.



A lo largo de todas las *releases* que 3GPP ha ido publicando el número de elementos funcionales que conforman el núcleo IMS se ha ido incrementando, así como la cantidad de puntos de referencia que conectan unos con otros. Hay elementos funcionales cuya diferencia entre ellos es mínima y esta sobre-fragmentación de las funciones ha dado lugar a un sistema muy complejo cuya implementación requiere de una inversión más que considerable por parte de los operadores. Esto es debido a que la tecnología IMS ya goza de cierta madurez y llega la fase de adaptación a los requerimientos que el propio mercado impone a nivel de servicios.

Núcleo IMS

Hay un consenso bastante extendido entre los operadores de telefonía móvil y los fabricantes de equipos del núcleo IMS que la especificación de éste se ha vuelto excesivamente compleja y es por ello por lo que, visto los servicios que más salida comercial tienen, como VoLTE, han solicitado que en futuras *releases* del 3GPP se realice una simplificación del propio núcleo.

Teniendo en cuenta esto último orientaremos el contenido de esta sección a la descripción de los elementos más básicos del núcleo IMS y que ya se están usando hoy en día por aquellos operadores que han optado por su implantación.

3.1.1. S-CSCF o *Serving Call Session Control Function*

El S-CSCF es el punto central y principal nodo de control de sesión SIP en una red IMS. Es responsable de mantener el proceso de registro, tomar decisiones de encaminamiento y mantenimiento del estado de sesión SIP, y el almacenamiento de los perfiles de servicio para usuarios activamente registrados.

Múltiples S-CSCF pueden existir concurrentemente en la red de un operador para garantizar balanceo de carga.

Para explicar con más detalle el papel del S-CSCF en el núcleo IMS, nos centraremos en cómo actúa cuando se dan los dos procesos más importantes: el registro de un cliente IMS (vía el mensaje SIP REGISTER) y el de establecimiento de una sesión (vía el mensaje SIP INVITE):

Registro y establecimiento de sesión en IMS

En secciones posteriores se presentan ejemplos de señalización intercambiada durante un registro y una llamada de VoLTE. Allí se ve más claramente el papel de los mensajes SIP REGISTER y SIP INVITE.

a) **En el proceso inicial de registro del usuario**, un usuario envía una petición de registro (SIP REGISTER) que es encaminada hacia un S-CSCF que previamente ha sido seleccionado por otro elemento del núcleo IMS que posteriormente veremos, el I-CSCF. En el intento inicial de registro, el S-CSCF descarga los datos de autenticación desde el HSS (vía la interfaz Cx) y responde a la petición de registro con un error de tipo *401 Unauthorized*. En esta respuesta, reta al UE a que proporcione en el siguiente intento la información de autenticación (un residuo calculado usando la contraseña).

b) **En el proceso final de registro del usuario**, el mismo S-CSCF recibirá (desde el I-CSCF vía la interfaz Mw) un segundo intento de registro conteniendo información de autenticación, la cual la compara con la que el propio S-CSCF ha calculado para saber si la autenticación es correcta. Si lo es, almacena la asociación entre la dirección IP de contacto que el UE usa y al menos una identificación pública (llamado IMPU) del usuario (la que ha usado para registrarse). Finalmente, el S-CSCF descarga del HSS un perfil de servicio (*Service Profile*) del usuario asociado al IMPU usado como parte del proceso de registro.

Interfaz Mw

La interfaz entre el CSCFs de un núcleo IMS es el Mw. Utilizada por los CSCF para reenviarse señalización SIP de registro o control de sesión (originada desde o destinada a un UE) entre ellos según sus criterios de encaminamiento. El 3GPP recomienda el protocolo SIP para su implementación (TS 23.517).

c) **En el proceso de encaminamiento de mensajes SIP de una nueva sesión de servicio multimedia**, el S-CSCF realizará una función u otra según si la llamada llega al usuario (*call terminating*) o es iniciada por el usuario (*call originating*):

Interconexión entre operadores con IMS

El modelo de referencia del 3GPP especifica que la señalización SIP entre dos operadores debe pasar por el IBCF, pero esto es así si dicha interconexión entre operadores ha sido específicamente implementada así. En caso contrario, la llamada se encamina vía redes heredadas usando el BGCF. De hecho, este es el caso más habitual aún hoy en día entre operadores de telefonía móvil que implementan VoLTE.

- *Terminating*: Si el mensaje SIP de *request* (principalmente SIP INVITE) es recibido por el S-CSCF del usuario destino, el S-CSCF encontrará la dirección IP asociada en el registro del usuario. Reenvía el mensaje al usuario final haciéndolo pasar antes por el P-CSCF tras el cual se encuentra dicho usuario (vía la interfaz Mw).

- *Originating*: consulta la cabecera *SIP Request-URI* del mensaje SIP de *request* para saber el siguiente salto (es decir a qué elemento del núcleo IMS ha de reenviarse). Este siguiente salto puede ser uno de los siguientes elementos:
  - A UE destino directamente (haciéndolo pasar por el P-CSCF correspondiente) **si el usuario llamado se encuentra registrado en el mismo S-CSCF**.
  - A un I-CSCF **si el usuario está registrado en otro S-CSCF** del mismo núcleo IMS.
  - A un SIP proxy específico llamado *Breakout Gateway Control Function* o BGCF **si el usuario destino es un alias no-IMS** (por ejemplo, un número telefónico). Éste, si ve que es de tipo telefónico, lo reenviará a

un *Media Gateway Control Function* o MGCF (pasarela de control hacia RTC/RDSI) de su elección.

– Al elemento fronterizo que comunica con otro núcleo IMS de otro dominio administrativo **si el usuario llamado se identifica con un alias de IMS**. Este elemento se llama *Interconnection Border Control Function* o IBCF.

– A un servidor de contenidos multimedia administrado por el propio operador **si la llamada es redirigida por ejemplo a un buzón de voz o contestador automático**. Este servidor es el MRF (*Media Resource Function*) que está dividido en dos bloques: el *Multimedia Resource Function Controller* o MRFC (recibe la señalización SIP) y, el *Multimedia Resource Function Processor* o MRFP (procesado de flujos multimedia).

d) Puede realizar **funciones de invocación de servicios externos que residen en SIP AS (servidores de aplicación)**. En este proceso el S-CSCF, antes de aplicar las funciones de encaminamiento descritas antes, consulta el perfil de servicio descargado desde el HSS del usuario. Este perfil incluye las iFC o *Initial Filter Criteria*, las cuales se usan para decidir a qué servidores de aplicaciones (SIP AS) y en qué orden se tienen que enviar los mensajes SIP de *request*. La interconexión entre el S-CSCF y los SIP AS se realizan vía la interfaz ISC. Además, el perfil de servicio puede incluir más instrucciones sobre qué tipo de política de comunicación necesita aplicar el S-CSCF (por ejemplo, podría indicar que un usuario está habilitado para utilizar componentes de audio, pero no de vídeo).

Interfaz ISC

La interfaz entre el S-CSCF y un SIP AS es el ISC. Utilizada por el S-CSCF y el AS para reenviar y recibir peticiones SIP (TS 23.218).

3.1.2. I-CSCF o *Interrogating Call Session Control Function*

El I-CSCF es usado para reenviar un mensaje SIP *request* inicial (como por ejemplo de registro SIP REGISTER o de inicio de sesión SIP INVITE) hacia un S-CSCF (vía la interfaz Mw) cuando el iniciador del mensaje no sabe a qué S-CSCF debería recibir dicho mensaje. De hecho, para llamadas entrantes desde otro dominio administrativo u operador, el I-CSCF es el punto de contacto dentro de la red del operador local para todas las conexiones destinadas a un suscriptor de este operador de red.

Para obtener la información sobre a qué S-CSCF se tiene que reenviar un mensaje SIP *request*, el I-CSCF contacta con el HSS (*Home Subscriber Server*) usando la interfaz Cx.

Interfaz Cx

La interfaz entre el S-CSCF /I-CSCF y un HSS es el Cx. Utilizada por el S-CSCF y el I-CSCF para consultar al HSS información de autenticación y autorización de usuario, perfil de suscripción, localización (S-CSCF asignado). El 3GPP recomienda usar el protocolo Diameter para su implementación (TS 29.229).

Siguiendo la misma filosofía que en la descripción de la anterior entidad funcional, las funciones más importantes que ha de realizar el I-CSCF se especifican a continuación:

a) **En el proceso inicial de registro del usuario**, el I-CSCF, al recibir el SIP REGISTER desde el P-CSCF, asigna un S-CSCF en función de las capacidades recibidas desde el HSS (el I-CSCF solicita al HSS qué opciones hay y selecciona el S-CSCF de una lista) y lo reenvía a dicho S-CSCF.

Interfaz Ma

La interfaz entre el I-CSCF y un SIP-AS es el Ma. Utilizada por el I-CSCF para reenviar peticiones SIP al AS con servicios públicos de identidades (PSI). El 3GPP recomienda usar el protocolo SIP para su implementación (TS 23.228).

b) **En el proceso de encaminamiento de mensajes SIP de inicio de sesión de servicio multimedia (SIP INVITE)**, el I-CSCF se encarga de obtener el nombre del siguiente salto (S-CSCF) hacia dónde dirigir (vía la interfaz Mw) dicho mensaje SIP. Se diferencian dos casos según si la red núcleo IMS al que pertenece el I-CSCF es el origen o el destino del inicio de la sesión:

- *Terminating*: Si el mensaje SIP de *request* (principalmente SIP INVITE) es recibido por el I-CSCF y éste se encuentra en la misma red o dominio que el usuario destino, el I-CSCF consulta el HSS para saber el S-CSCF al cual el usuario destino está asociado. Para hacer esta consulta, se basa en la cabecera *SIP Request-URI* que el propio SIP INVITE lleva.

- *Originating*: Para que el I-CSCF reciba un mensaje SIP de *request* estando en la red de origen el mensaje de *request* debe haberse originado desde un servidor SIP de aplicación (vía una interfaz llamada Ma) en nombre de un usuario y dicho servidor no sabe el S-CSCF del usuario que ha originado la llamada. En este caso concreto el I-CSCF consultará el HSS para saber en qué S-CSCF está registrado el usuario que origina la llamada y enviar el mensaje SIP a dicho S-CSCF.

c) Proporcionar **funcionalidad THIG (*Topology Hiding Inter-network Gateway*)** de manera opcional. Otro operador que quiera enviar señalización SIP hacia el dominio local, lo enviará al I-CSCF como si fuera un proxy, ya que será el único elemento del núcleo IMS visible desde el exterior (desde otros operadores). El I-CSCF puede actuar como un elemento SBC (*Session Border Controller*, concepto definido en la siguiente sección) solo a nivel de señalización SIP para la interfaz entre dos dominios o redes NGN (interfaz NNI).

3.1.3. P-CSCF o *Proxy Call Session Control Function*

El **P-CSCF** es el primer punto de contacto dentro de IMS para los usuarios adheridos a una red de acceso y es la razón por la que se le considera un elemento de control fronterizo (*Session Border Controller*) con el usuario (interfaz UNI).

En realidad, el concepto de *Session Border Controller* se aplica en todo aquel punto de la red NGN en el que haya una frontera de dominio administrativo (es decir, tanto en la interfaz UNI, donde UE y dominio IMS se unen, como en la interfaz NNI, donde dos dominios IMS se unen).

Session Border Controller o SBC

Un *Session Border Controller* o SBC es un elemento colocado en las fronteras administrativas de una red gestionada o dominio. Aborda los problemas que surgen de la provisión de servicio multimedia basado en sesiones IP. Estos problemas son la **seguridad** donde se hace control de admisión de llamada en las fronteras de la red para garantizar QoS del tráfico que entra y sale, se evita el abuso en el uso del servicio y se realizan tareas de protección de la privacidad del operador y el usuario. También comprenden funciones para solventar los problemas del uso de protocolos como SIP en presencia de un **cortafuegos o NAT** (SIP ALG o *Application Level Agreement*) o funciones de **monitorización regulatorias** como la intercepción de tráfico por ley (*lawful interception*), **facturación y monitorización del servicio**. Un SBC puede tener entidades funcionales separadas para señalización y medios.

Así pues, todo el tráfico de señalización IMS que parta de o llegue al UE antes deberá haber pasado por el P-CSCF. Esta interfaz de señalización entre estos dos elementos es llamada Gm y el UE pondrá siempre la dirección IP del P-CSCF como destino, ya que éste hace de proxy para todas las transacciones SIP.

Interfaz Gm

Interfaz entre UE y P-CSCF para intercambiar mensajes de señalización SIP de IMS (registro, control de sesiones y transacciones). El 3GPP recomienda usar el protocolo SIP para su implementación (TS 23.002).

Las funciones más importantes que ha de realizar el P-CSCF se especifican a continuación:

a) **En el proceso inicial de registro del usuario**, el P-CSCF deberá reenviar la petición de SIP REGISTER llegada desde el UE al elemento del núcleo IMS que se encarga de redirigir el mensaje de registro al S-CSCF asignado, y este elemento es el I-CSCF. Para ello observa la cabecera del mensaje SIP, en concreto la parte que describe el dominio en el SIP URI al cual pertenece el usuario. A partir de este dominio puede descubrir a qué I-CSCF (es decir, su *hostname*) tiene que reenviar el SIP REGISTER (ya sea resolviendo vía DNS o consultando alguna tabla preconfigurada).

Papel del I-CSCF

Cuando un UE se registra por primera vez, el P-CSCF no sabe a qué S-CSCF debe redirigir el SIP REGISTER y por defecto ha de encontrar al menos un I-CSCF al cual reenviar dicho mensaje. En el caso de ser un mensaje SIP de inicio de llamada (SIP INVITE) el P-CSCF ya sabrá a qué S-CSCF ha de reenviar el mensaje ya que esta información ya habrá quedado almacenada en la fase de registro. En este último caso, el I-CSCF no participa en absoluto.

b) **En el proceso final de registro del usuario**, el P-CSCF deberá almacenar información del registro en sí que relacione unívocamente al UE con el S-CSCF asignado. Por ejemplo, almacena la información de contacto del UE (IP asignada) y la dirección del S-CSCF, así como los identificadores públicos del usuario (IMPUs) que el S-CSCF ha asociado en el registro.

c) **Al iniciar o recibir el UE una nueva sesión de servicio multimedia**, el P-CSCF deberá verificar que los campos de la cabecera del mensaje SIP INVITE contengan los valores acordes a la información almacenada durante la fase de registro. Una vez el mensaje ha sido verificado, se encargará de redirigir los mensajes SIP al S-CSCF asignado o al UE (según si el UE es el iniciador o el receptor de dicha sesión) vía una interfaz llamada Mw.

Seguridad entre UE y P-CSCF

Esto se consigue tras el primer intento de registro SIP cuando el UE recibe respuesta con un código de error 401 originado por el S-CSCF correspondiente, el cual incluye un *Authentication Vector* en el que hay dos claves: IK o *Integrity Key* y el CK o *Cipher Key*, que deberá usar el P-CSCF para negociar asociaciones de seguridad IPSec. Así pueden aplicar protección de confidencialidad e integridad para el resto de la señalización SIP.

d) **Al hacer el papel de elemento fronterizo con el UE** (interfaz UNI), puede ofrecer **funcionalidades de garantía de integridad y confidencialidad** de toda la información de señalización intercambiada entre el UE y el núcleo IMS (sobretodo en el caso de que el UE se conecte usando una red de acceso no gestionada por el propio operador o susceptible de ser escuchada por terceros). Esta funcionalidad la realiza estableciendo una conexión segura entre el UE y el P-CSCF ya sea usando una conexión IPSec o TLS.

e) Tiene **un papel muy importante en la garantía de la QoS de los servicios invocados**. Al ser un SBC, procesa la información relacionada con los recursos multimedia asociados a una sesión (como, por ejemplo, los requerimientos en bits por segundos asociados al uso de un codificador de voz en concreto). Esta información de recursos viene implícita o explícitamente incluida en la señalización SIP que el propio UE genera y el P-CSCF la sintetiza para enviarla a la subcapa de control de transporte vía la interfaz Rx. Esta información de recursos multimedia puede incluso ser manipulada por el propio P-CSCF (a modo de SBC) para realizar funciones de transcodificación y así resolver problemas de incompatibilidad entre UEs (apoyándose en elementos en la capa de transporte que procesen el tráfico de voz).

f) Puede opcionalmente realizar funciones de **compresión y descompresión de los mensajes SIP** que provienen del UE si y sólo si la conexión establecida entre el cliente IMS (UE) y el P-CSCF es soportada y así se ha negociado.

P-CSCF y UE en itinerancia

En el caso de ser un I-CSCF del mismo dominio que el P-CSCF, el SIP REGISTER se reenvía a este elemento. Si el I-CSCF es de distinto dominio (en caso de itinerancia) el SIP REGISTER se envía al I-CSCF vía el correspondiente elemento de control fronterizo o SBC de la red visitada, que en este caso es la entidad IBCF (usando una interfaz llamada Mx)

g) Detectar y **gestionar las peticiones de sesión de emergencia** (selección de un S-CSCF dedicado exclusivamente para emergencias, llamado E-CSCF).

Cuando el P-CSCF recibe un inicio de llamada (SIP INVITE que podría provenir incluso de un UE no registrado) el alias (SIP URI del tipo sip:usuario@dominio.com) o número de teléfono de destino (Tel URI del tipo tel: 933219876) se compara con una lista preconfigurada de teléfonos de emergencia (normalmente es la misma con independencia del país gracias acuerdos internacionales, como el número 112).

h) Como ya hemos mencionado antes, opcionalmente puede también actuar **como pasarela de señalización (entre la interfaz W2 basado en web-socket y la interfaz Mw basado en SIP) para llamadas hechas desde el UE usando tecnología WebRTC**. En este caso se le llamaría eP-CSCF (*enhanced* P-CSCF).

3.2. Componentes de almacenaje de información de suscripción

A continuación, vamos a explicar aquellas entidades especializadas en el almacenaje de suscripciones de usuario y que son clave en la provisión de servicios.

3.2.1. HSS o *Home Subscriber Server*

Es la base de datos principal de suscriptores para IMS. Contiene información de suscripción de cada usuario y la distribuye a diferentes entidades funcionales del núcleo IMS o servidores de aplicaciones (SIP AS o *SIP Application Servers*).

La información de suscripción que el núcleo IMS usa contiene principalmente lo siguiente:

- **Información de autenticación del suscriptor a nivel de registro en el núcleo IMS**, la cual está compuesta por al menos una identidad privada o IMPI y una contraseña.

- **Relación entre las distintas identidades privadas (IMPI) y públicas (IMPU)** llamadas *Implicit registration set*.

- **Información de invocación de servicios en SIP AS o *Service Triggering Data***, la cual está compuesta por los *Service Profiles* asociados a los IMPUs y que contienen las reglas de orquestación de mensajes SIP hacia los distintos SIP AS. Estas reglas se llaman *initial filter criteria* o IFCs.

Información relacionada a los servicios proporcionados al usuario, información de tarificación, máximo número de llamadas por sesión, máximo número de sesiones simultáneas, componentes multimedia habilitados (si puede usar vídeo y/o audio en una llamada), etc.

Un **IRS o *Implicit Registration Set*** es la asociación implícita de varias identidades públicas (IMPU) con una identidad privada (IMPI). Es decir, que si un usuario se registra en el núcleo IMS usando la identidad privada o IMPI y una identidad pública o IMPU en concreto, el usuario podrá ser llamado usando tanto el IMPU que ha usado en el registro como todos los IMPUs extras asociados en dicho IRS. Estas asociaciones entre identidades se vuelcan desde el HSS al S-CSCF en la fase de registro para que éste último pueda identificar dichos IMPUs como válidos.

Otras funciones del HSS no relacionadas con IMS

En un contexto de telefonía móvil, el HSS también realiza una serie de funciones. Con el objeto de interaccionar con los dominios de conmutación de paquetes (formado por el propio núcleo IMS y el EPS) y conmutación de circuitos, la HSS contiene funcionalidades de *Home Location Register* (HLR) en redes móviles LTE y *Authentication Center* (AUC), tal y como define el 3GPP.

Esta información de suscripción puede ser proporcionada directamente a través de la interfaz de control Cx (al I-CSCF o S-CSCF) o indirectamente aprovechando la misma señalización SIP de alguna transacción en curso (al P-CSCF o el UE).

Interfaz Sh

Interfaz entre SIP AS y el HSS utilizada por el AS para consultar al HSS información de autenticación y autorización de usuario, perfil de suscripción, localización (S-CSCF asignado). El 3GPP recomienda usar el protocolo Diameter para su implementación (TS 29.329).

Los SIP AS también pueden usar el HSS para almacenar y obtener información específica del servicio que proporcionan (vía la interfaz Sh) a un usuario. Esta información se clasifica en dos tipos en función de si el formato de dicha información no está estandarizado (*transparent*) o sí lo está (*non-transparent*). El operador podrá configurar una lista de SIP AS autorizados, así como políticas de privacidad para los usuarios.

El HSS es capaz de manejar otros identificadores públicos distintos a los IMPUs. Son conocidos como identificadores de servicio o PSI (*Public Service Identifier*) de acuerdo con las especificaciones de 3GPP.

Un **PSI o *Public Service Identifier*** identifica todo aquello que pueda ser receptor de un mensaje petición SIP y no es un usuario (para el cual se usaría un IMPU). Con lo cual, un PSI puede identificar cualquier recurso de un servicio provisto por un servidor de aplicación (AS), el cual puede ser el propio servicio en sí. Como ejemplos de recursos, un PSI puede identificar un contenido en concreto, una conferencia ya predefinida, una habitación de chat, etc. Un PSI puede identificar también por ejemplo a todo un grupo de usuarios.

A continuación, se resume la participación del HSS en los procesos de registro y encaminamiento de mensaje SIP durante el establecimiento de sesiones:

Métodos de autenticación en IMS

El HSS debe soportar diversos modelos de autenticación: IMS AKA, IETF HTTP *Digest* e IMS SSO.

a) **En el proceso inicial de registro del usuario**, se le asigna un S-CSCF. Antes de esta asignación, la HSS decide si el usuario está autorizado a registrarse en el subsistema IMS basándose en las identidades públicas (IMPU) recibidas en la petición de registro (comunicadas por el I-CSCF vía la interfaz Cx), en los datos de configuración de la HSS y en la información de usuario almacenada. El HSS permite el proceso de asignación de S-CSCF comunicándole al I-CSCF la identidad del S-CSCF en el que el usuario está registrado, o bien un conjunto de capacidades que serán empleadas por el I-CSCF para seleccionar el más adecuado. El HSS almacena la información del S-CSCF asignado a dicho usuario. Finalmente, el S-CSCF solicita al HSS información de autenticación para retar al UE a autenticarse en un segundo intento de registro.

b) **En el proceso final de registro del usuario**, el S-CSCF, una vez que ha autenticado correctamente al usuario, solicita al HSS el volcado de la lista de IMPUs asociados en el IRS (si lo hubiera) y la lista de IFCs asociados al *service profile* del IMPU o grupo de IMPUs usados.

c) El HSS **participa en el establecimiento de la sesión IMS** cuando el usuario la inicia. El HSS no encamina mensajes SIP, pero devuelve al I-CSCF vía la interfaz Cx el hostname del S-CSCF asignado a un usuario en el caso de que la identidad pública involucrada en la sesión haya sido registrada con anterioridad. Si la identidad pública (IMPU) no está registrada, la HSS indica al I-CSCF que el usuario no es alcanzable.

3.2.2. SLF o *Subscriber Location Function*

Normalmente un operador distribuye la información de los suscriptores en múltiples HSS. En una red con esta característica, ni el I-CSCF ni el S-CSCF conocen en cuál de estas HSS se encuentra la información que necesitan consultar. Por lo tanto, deben contactar primero con el SLF.

El SLF debe proveer una funcionalidad de encaminado que permita que otras entidades descubran qué nodo HSS contiene la información de suscripción de un determinado usuario (proporcionando el IMPU), otorgando al operador la flexibilidad de distribuir sus usuarios libremente entre varias HSSs. Se precisa entonces de la implementación de una entidad funcional como la del SLF y de sus puntos de referencia llamados Dx (conexión con S-CSCF y I-CSCF) y Dh (conexión con servidores de aplicaciones).

Interfaz Dx

Utilizada por el S-CSCF y el I-CSCF para consultar al SLF sobre la localización del HSS que contiene la información de suscripción de un usuario. El 3GPP recomienda Diameter para su implementación (TS 29.229).

Interfaz Dh

Utilizada por el AS para consultar al SLF sobre la localización del HSS que contiene la información de suscripción de un usuario. El 3GPP recomienda Diameter para su implementación (TS 29.328).

3.3. Mecanismos de garantía de recursos y QoS en red de transporte

En las redes NGN se han especificado dos mecanismos de reserva de recursos que se aplican tanto en la red de acceso como troncal de transporte: modo *push* y modo *pull*.

Modo *push*

La Figura 11 nos muestra un ejemplo del proceso paso a paso de reserva de recursos y garantía de QoS correspondiente al modo *push*, y en concreto de una llamada de VoLTE. Hay que tener en cuenta que, siguiendo el orden de los pasos, la reserva se dispara desde la capa de control de servicio (en este caso el núcleo IMS), con el P-CSCF si es la red de acceso y posteriormente se traduce en la instalación de políticas de QoS (en el caso de LTE, reglas PCC) sobre la capa de procesado de transporte.

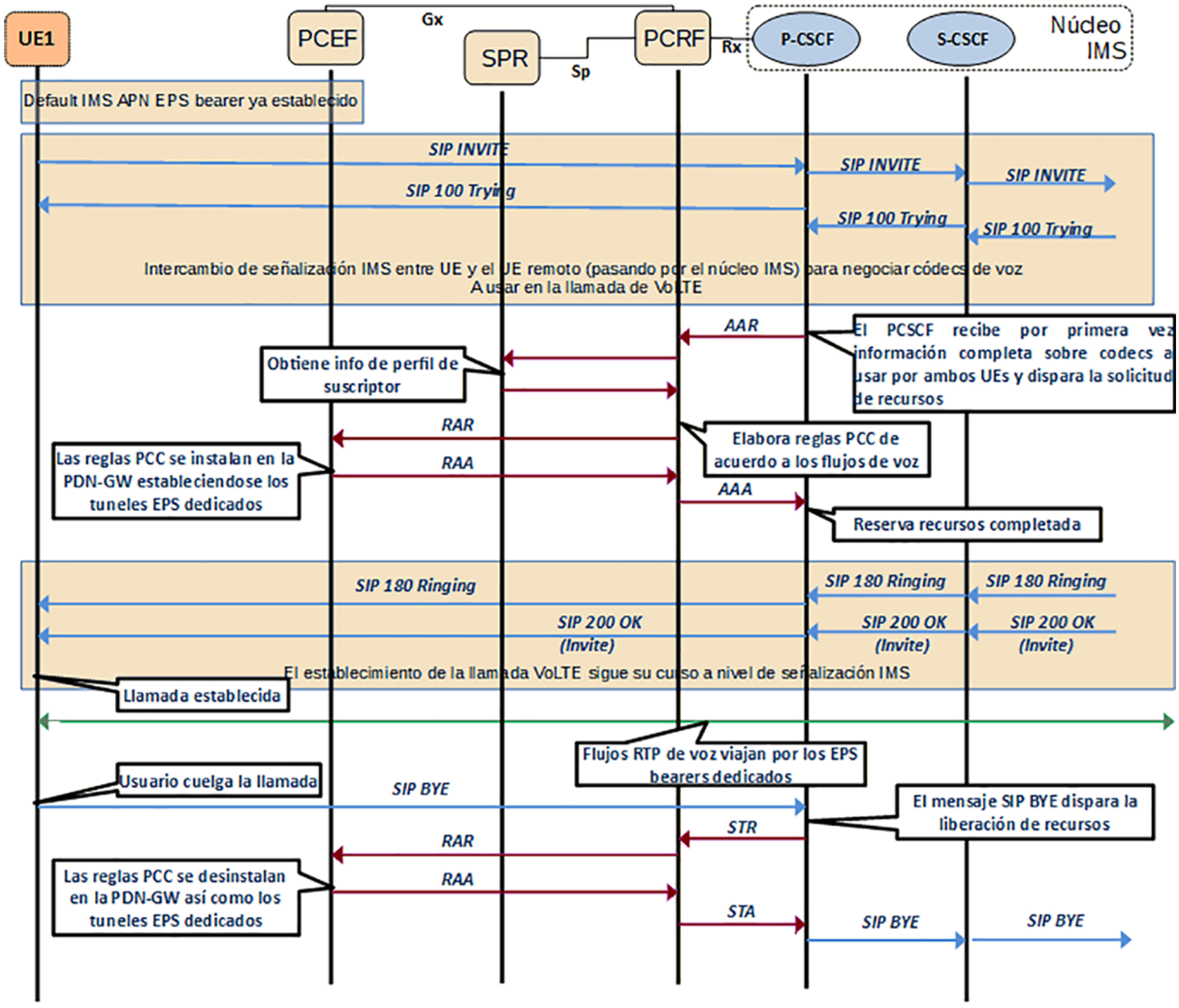
Entre el P-CSCF (capa de servicio) y el PCRF (en la capa de transporte) la interfaz de control está basada en Diameter y la especificación del 3GPP lo llama Rx (3GPP TS 29.214). En dicha figura veréis que el P-CSCF, tras haber evaluado la negociación de los códecs de voz entre ambos UEs (realizado con el protocolo SDP), extrae dicha información y la envía en un mensaje AAR (*Authorization Authentication Request*) al PCRF. Esperará hasta que éste le responda con un AAA (*Authorization Authentication Answer*) para saber si la reserva solicitada ha acabado exitosamente o no para continuar encaminando los mensajes SIP de la llamada o directamente cancelarla (enviando a ambos extremos de la llamada un mensaje de SIP CANCEL).

Negociación de parámetros multimedia de llamada

La información de negociación de parámetros multimedia para la comunicación (códecs de voz y video, puertos UDP a usar, etc.) se realiza con el protocolo SDP, el cual está integrado en algunos de los mensajes SIP intercambiados durante el establecimiento de la llamada. Dichos parámetros los proponen siempre los UE.

El PCRF, antes de responder al AAR enviado por el P-CSCF tendrá que evaluar la información de perfil del usuario a nivel de capa de transporte para decidir si instala una regla PCC o no en el PCEF (PDN-GW). En caso afirmativo, envía un mensaje Diameter RAR (*Re-Auth Request*) vía la interfaz Gx (3GPP TS 29.212) solicitando la instalación de la regla PCC y esperará la respuesta (afirmativa o negativa) en el mensaje RAA (*Re-Auth Answer*) sobre el procedimiento de instalación de la regla.

Figura 11. Ejemplo de mecanismo de reserva de recursos en modo *push*.



Modo *pull*

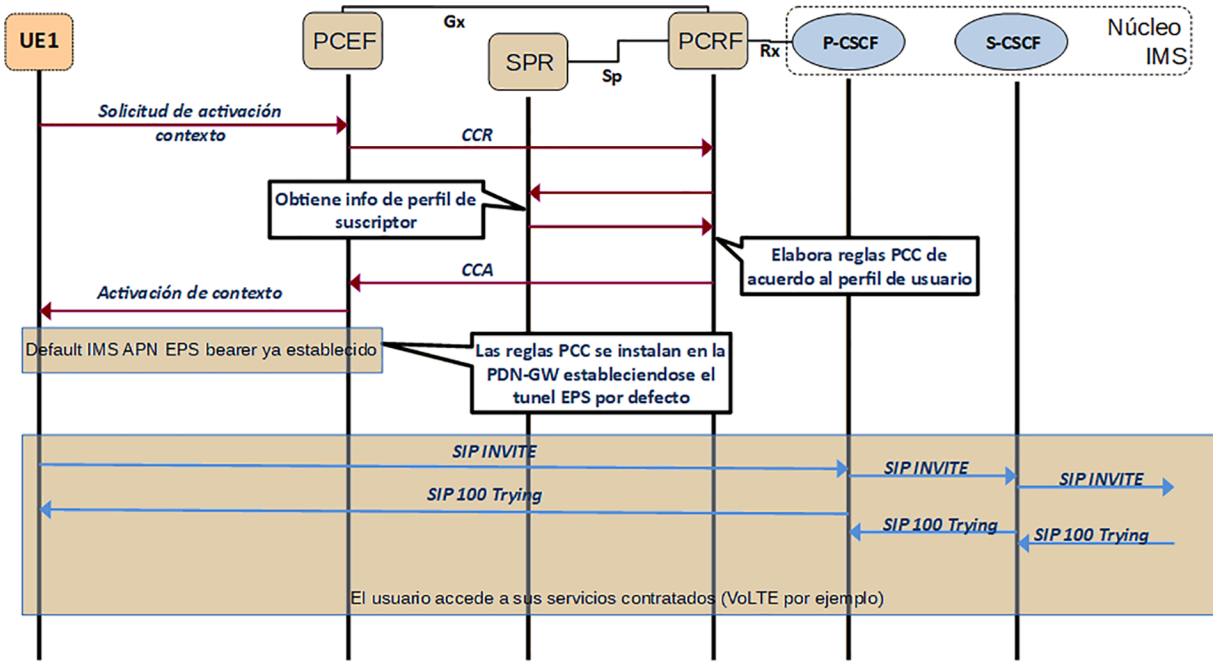
La Figura 12 nos muestra un ejemplo del proceso paso a paso de reserva de recursos y garantía de QoS correspondiente al modo *pull*, en concreto cuando un UE se enciende y se adhiere a la red LTE iniciando una sesión EPS.

Modo *pull*

Un UE puede iniciar también la reserva de recursos durante el establecimiento de una llamada VoLTE mediante la solicitud de establecimiento de un túnel EPS dedicado para la voz.

Cuando el PCEF recibe la solicitud desde el UE, éste dispara una petición de instalación de una regla PCC al PCRF, el cual consulta el perfil de usuario a nivel de transporte y toma las decisiones pertinentes sobre el establecimiento de la regla PCC que posibilita el establecimiento del túnel EPS por defecto asociado al APN IMS. Dicha solicitud se realiza vía la interfaz Gx vía un intercambio de mensajes CCR/CCA (*Credit Control Request/Answer*) entre el PCEF y el PCRF.

Figura 12. Ejemplo de mecanismo de reserva de recursos en modo *pull*.



Los mensajes CCR también se usan para transmitir eventos al PCRF relacionados con la conectividad del UE (por ejemplo, si el UE se ha apagado) y el *accounting* de un servicio en concreto. El PCRF puede por un lado retransmitir dichos eventos al P-CSCF (siempre y cuando éste lo hubiera solicitado en la solicitud de recursos en modo *push*) y por otro tomar decisiones sobre alteraciones en las reglas PCC afectadas por dicho evento (puede disparar incluso la desinstalación de reglas PCC).

Transmisión de eventos

Los mensajes CCR/CCA están definidos tanto en la especificación de la interfaz Rx como en la del Gx. En este último se usa tanto para solicitar reserva de recursos en modo *pull* como para transmitir eventos.

3.4. Protocolos básicos empleados en las redes NGN e IMS

Como hemos visto en las descripciones de los puntos de referencia en anteriores apartados, los protocolos que dominan la capa de servicio son SIP, Diameter. En este apartado veremos las principales características de cada uno.

3.4.1. Protocolo SIP

Session Initiation Protocol o SIP (Protocolo de Iniciación de Sesión) es un protocolo de señalización definido por el IETF (*Internet Engineering Task Force*) que permite el establecimiento, la liberación y la modificación de sesiones multimedia (RFC3261). Este protocolo hereda ciertas funcionalidades de los protocolos HTTP, utilizados para navegar sobre la WEB y SMTP, para transmitir mensajes electrónicos (e-mails). SIP se apoya sobre un modelo transaccional cliente/servidor como HTTP. Como en SMTP, el formato de un mensaje SIP está basado en cabeceras o *headers,* las cuales están expresadas en texto. El protocolo SIP puede usarse bajo TCP, UDP o SCTP.

Para temas de direccionamiento, SIP utiliza el concepto *Uniform Resource Identifier* o SIP URI, el cual es parecido a una dirección e-mail (usuario@dominio.com). Cada participante en una red SIP es entonces localizable por medio de una SIP URI.

Es importante resaltar que SIP es un protocolo de señalización para iniciar, modificar y liberar sesiones multimedia pero no es un protocolo de reserva de recursos y, en consecuencia, no puede por sí solo asegurar la calidad de servicio extremo a extremo. Se trata de un protocolo de control de llamada y no de control del medio. Como ya hemos mencionado antes, emplea el protocolo SDP (*Session Description Protocol*) para intercambiar parámetros de capacidad y de los usuarios en términos de codificación y ancho de banda de los flujos multimedia que se intercambiarán. Estos flujos se apoyan en el protocolo RTP/RTCP (*Real Time Protocol / Real Time Control Protocol*).

A continuación, veremos las entidades que define el protocolo SIP. Estas entidades describen los actores que pueden aparecer en toda comunicación SIP. Posteriormente, veremos cómo son los mensajes SIP junto con los tipos de peticiones y respuestas que el protocolo especifica. Finalmente, veremos las extensiones a la especificación SIP del IETF que IMS ha introducido.

Entidades SIP

SIP define dos tipos de entidades: los clientes y los servidores. Más concretamente, las entidades definidas por SIP son:

- **Servidor Proxy** (*Proxy Server*): recibe solicitudes de clientes que él mismo trata o encamina hacia otros servidores después de haber realizado ciertas modificaciones sobre estas solicitudes. Este elemento se encuentra implementado en diversos elementos del núcleo IMS como el P-CSCF, I-CSCF, S-CSCF, E-CSCF y en definitiva en cualquier elemento que se encargue de encaminar mensajes SIP.

- **Servidor de Redirección** (*Redirect Server*): se trata de un servidor que acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias di-

recciones de red y las devuelve al cliente. De manera contraria al Proxy Server, el *Redirect Server* no encamina las solicitudes SIP. En el caso de la devolución de una llamada, el Proxy Server tiene la capacidad de traducir el número del destinatario en el mensaje SIP recibido en un número de reenvío de llamada y encaminar la llamada a este nuevo destino de manera transparente para el cliente de origen; para el mismo servicio, el *Redirect Server* devuelve el nuevo número (número de reenvío) al cliente de origen quien se encarga de establecer una llamada hacia este nuevo destino.

- **Agente Usuario** (*User Agent*) o UA: se trata de una aplicación sobre un equipo de usuario que emite y recibe solicitudes SIP. En un contexto IMS, este elemento estaría localizable por ejemplo en un UE en modo de cliente SIP o también en un MGCF donde la llamada SIP se transforma en una llamada a RDSI o RTC.

- **El Registrador** (*Registrar*): se trata de un servidor que acepta las solicitudes SIP REGISTER. SIP dispone de la función de registro de los usuarios. El usuario indica por un mensaje REGISTER emitido al Registrar, la dirección donde es localizable (dirección IP). El Registrar actualiza entonces una base de datos de localización. El registrador es una función asociada a un *Proxy Server* o a un *Redirect Server*. Un mismo usuario puede registrarse sobre distintas UA SIP, en este caso, la llamada le será entregada sobre el conjunto de estas UA. Este elemento se encontraría implementado en el S-CSCF en el núcleo IMS y la base de datos de localización sería implementada en el HSS.

Mensajes SIP

A continuación, vamos a ver qué tipos de mensajes y qué funciones desempeñan en la especificación del protocolo SIP. Primero echaremos un vistazo a la estructura típica de la cabecera SIP y los tipos de peticiones y respuesta que contempla la especificación.

Cabecera SIP

Un mensaje SIP está compuesto por una serie de campos, todos basados en texto. El orden en que aparecen es indistinto e incluso un mismo campo puede aparecer varias veces conteniendo valores diferentes. En SIP, cuando hay más de un campo repetido, sí que puede importar en qué orden aparecen los campos introducidos.

A continuación, mostramos un ejemplo de una cabecera SIP (sin cabecera SDP):

```
INVITE sip:bob@iptel.org SIP/2.0
Via: SIP/2.0/UDP 176.54.75.23:5040;rport
Max-Forwards: 10
```

```
From: "jiri" <sip:jiri@iptel.org>;tag=76ff7a07-c091-4192-84a0-
d56e91fe104f
To: Bob <sip:bob@iptel.org>
Call-ID: d10815e0-bf17-4afa-8412-d9130a793d96@176.54.75.23
CSeq: 2 INVITE
Contact: <sip:jiri@176.54.75.23:5040>
User-Agent: Windows RTC/1.0
Proxy-Authorisation: Digest username="jiri", realm="iptel.org",
algorithm="MD5", uri="sip:jiri@bat.iptel.org",
nonce="3cef753900000001771328f5ae1b8b7f0d742da1feb5753c",
response="53fe98db10e1074
b03b3e06438bda70f"
Content-Type: application/sdp
Content-Length: 451
v=0
o=jku2 0 0 IN IP4 176.54.75.23
s=sesión
...
```

En la primera línea encontramos la palabra INVITE, que es el nombre del método SIP del mensaje. En este caso se trata de un mensaje de tipo petición (*Request*) para el inicio de sesión. En el subapartado siguiente podéis ver el resto de los métodos SIP que existen. En lugar del método también puede ir el código o número cuando se trata de un mensaje de respuesta. Los códigos de respuesta los podéis encontrar más adelante. A continuación, aparece un SIP URI representando el destinatario de dicho mensaje (se le llama *Request* URI). En este caso se trata del equipo con *hostname* iptel.com.

Una petición SIP puede contener uno o más campos *Via:* que son usados para registrar el camino que dicha petición realiza hasta su destino. Luego son usados para encaminar las respuestas exactamente de la misma manera. En el ejemplo vemos que hay un solo campo *Via:* y nos dice que el cliente SIP (o también llamado User Agent) se ejecuta en un PC con IP 176.54.75.23 y usa el puerto 5040.

Los campos *From:* y *To:* al igual que en SMTP contienen identificadores del originador de la petición (usuario llamante) y el destinatario (usuario llamado).

El campo *Call-ID:* es un identificador del diálogo SIP y su función es identificar mensajes pertenecientes a la misma llamada.

El campo *CSeq:* es usado para mantener el orden de las peticiones. Se utiliza en las respuestas también para identificar a qué petición hace referencia.

La cabecera *Contact:* contiene la dirección IP y el puerto sobre el cual el solicitador está esperando posteriores peticiones enviadas por el usuario llamado.

Las otras cabeceras del ejemplo no son importantes y no vale la pena describirlas. No obstante, el protocolo SIP contempla otras cabeceras como *Route:* o *Record Route:* indican información de encaminamiento (salto a salto) del mensaje SIP.

La cabecera *Message:* está delimitada del cuerpo del mensaje por una línea vacía. El contenido del cuerpo del mensaje puede ser otro protocolo que aporta información adicional sobre la sesión. Ejemplos de estos protocolos son SDP (*Session Description Protocol*) y XML.

Métodos SIP

Los métodos SIP pueden dividirse en dos tipos: peticiones y respuestas. A continuación, se muestra una lista de las peticiones:

Tabla 2. Métodos SIP (peticiones).

Método	Descripción
INVITE	Enviado desde el terminal UA llamante al UA llamado. Indica que un cliente está siendo invitado a participar en una sesión de llamada.
ACK	Confirma que el cliente ha recibido una respuesta final a una petición INVITE (respuesta con códigos 2xx, 3xx, 4xx, 5xx y 6xx). No se recibe respuesta al enviar un ACK.
BYE	Enviado por el llamante o el llamado para terminar una sesión.
CANCEL	Cancelar cualquier petición pendiente de respuesta o cualquier transacción.
OPTIONS	Solicita a otro UA o a un servidor proxy qué capacidades tienen (métodos soportados, los tipos de contenidos, las extensiones, los códecs, etc. sin tener que provocar el "ringing" de la otra parte).
REGISTER	Usado por un UA para notificar a una red SIP de su dirección IP actual (*Contact URI* en la cabecera) y del URI a los que se debería encaminar las peticiones.
PRACK	ACK provisional. Es como un ACK para respuestas provisionales con código 1xx (RFC 3262).
SUBSCRIBE	Suscripción a un evento de notificación enviados desde un notificador (RFC 3265).
NOTIFY	Usado para notificar a las entidades suscriptoras sobre un evento de actualización de registro (RFC 3265).
PUBLISH	Enviado por un cliente para publicar un evento a un servidor proxy.
INFO	Envía información a mitad de sesión que no modifica el estado de dicha sesión (RFC 2976). Entre los ejemplos de información se encuentran los dígitos DTMF, las informaciones relativas a la tasación de una llamada, etc.
REFER	Un UA lo puede usar para instar a otro UA a que inicie una petición SIP (normalmente un SIP INVITE) hacia un tercer UA. Permite emular distintos servicios o aplicaciones incluyendo la transferencia de llamada (RFC 3515).

Método	Descripción
MESSAGE	Transporta mensajes instantáneos de texto usando SIP. El mensaje SIP MESSAGE puede transportar varios tipos de contenidos basándose sobre la codificación MIME (RFC 3428).
UPDATE	Modifica el estado de la sesión sin cambiar el estado del diálogo SIP. Permite a un cliente SIP actualizar los parámetros de una sesión multimedia (flujos multimedia y sus códecs). El método UPDATE puede ser enviado antes de que la sesión haya sido establecida (RFC 3311), es decir antes de recibir el 200 OK correspondiente al SIP INVITE que ha iniciado la sesión.

Respuestas SIP

Una respuesta es enviada por un servidor SIP a un cliente y tiene la siguiente estructura:

```
SIP VERSION (space)STATUS CODE (space)EXPLANATION
```

El STATUS CODE es un código numérico usado por el receptor para identificar el estatus de la petición. Está formada por tres dígitos seguidos por una descripción textual del código.

El STATUS CODE está dividida por 6 familias diferentes donde el primer dígito indica la clase del código como es mostrado en la siguiente tabla.

Tabla 3. Métodos SIP (respuestas).

Código	Descripción	Ejemplo
1xx	Respuestas provisionales/informacionales	100 Trying, 180 Ringing
2xx	Respuestas exitosas	200 OK
3xx	Respuestas de redirección	302 Moved Temporarily, 305 Use Proxy
4xx	Respuestas de error de cliente	401 Unauthorized, 408 Request Timeout
5xx	Respuestas de error de servidor	500 Server Internal Error, 503 Service Unavailable
6xx	Respuestas de error globales	600 Busy Everywhere, 603 Decline

Extensiones para IMS

El protocolo SIP fue elegido por el 3GPP como base para la señalización de IMS. No obstante, había muchos huecos entre el protocolo SIP de base definido por IETF y las características requeridas para soportar las prestaciones de IMS al completo. Para resolver este problema, el 3GPP definió docenas de extensiones SIP específicas para redes IMS. Colectivamente, estas extensiones comprenden el protocolo SIP IMS definiendo un perfil propio de SIP. El protocolo SIP IMS está definido en el estándar del 3GPP TS 24 229.

Estas extensiones, como el control de llamada extendido, la presencia o la mensajería instantánea, extienden la funcionalidad de SIP sobre las redes IMS. Este nuevo perfil de uso del protocolo SIP para IMS representa el más importante en la industria de las telecomunicaciones y es de manera exclusiva el más apropiado para las redes NGN.

Para ilustrar la inherente complejidad del SIP IMS y todas sus extensiones, vamos a ver por encima las extensiones más importantes:

1) SigComp: define cómo comprimir los datos en texto de la señalización SIP, los cuales pueden ser muy extensos y problemáticos de transmitir, causando retardos. SigComp solventa los retos de retardos de ida y vuelta de la señalización, así como la vida de la batería de los UE móviles. Más información acerca de SigComp se puede encontrar en el RFC 3320.

2) Cabeceras privadas o *P-headers*: además de las cabeceras estándar, el 3GPP definió cabeceras adicionales dirigidas a solventar problemas específicos de la red IMS, como obtener información sobre la red de acceso y la red visitada (en itinerancia) así como determinar la identidad del llamante. Más información acerca de los *P-headers* se puede encontrar en los RFC 3455 y RFC 3325.

3) Negociación a nivel de seguridad o Security Agreement: especifica cómo negociar las capacidades de seguridad para múltiples tipos de terminal. Más información sobre *Security Agreement* se puede encontrar en el RFC 3329.

4) AKA-MD5: determina cómo terminales y redes son autenticados utilizando mecanismos ya definidos (por ejemplo, ISIM) así como intercambio de claves específicas. Más información sobre AKA-MD5 se puede encontrar en el RFC 3310.

5) IPSec[1]: utilizado en varios interfaces IMS (como el Gm) entre diferentes redes IMS para garantizar confidencialidad e integridad de los datos. IMS usa IPSec en modo transporte, en oposición al estándar usado en servicios VPN.

(1)Un enlace IPSec entre dos terminales puede establecerse en dos modos: modo túnel para VPNs *site-to-site* o *LAN-to-LAN* y en modo transporte para conectar un host con otro host que ejerce de concentrador de VPN. Estas VPN se llaman VPN en modo acceso remoto.

6) Autorización de medios o *Media Authorization*: Se asegura que solo los recursos de medios autorizados son utilizados. Se puede encontrar información más detallada en el RFC 3313.

7) Registro en movilidad o *Mobile Registration*: En redes IMS, el proceso de registro del terminal es más complicado ya que incluye varias extensiones de seguridad y debe gestionar registros desde una red visitada. En el RFC 3608 y RFC 3327 se define la sintaxis y el uso por parte de las entidades SIP de las cabeceras *Service-route* y *Path*.

8) *Reg-event Package*: usado por el terminal y el P-CSCF para saber el estatus de registro del terminal en la red. IMS IPv6 prefiere redes IPv6, que ofrece distintas ventajas. Permite un rango más amplio de direcciones y contiene

funcionalidad IPSec integrada que puede eliminar la necesidad de cortafuegos y NAT para las entidades. Información más detallada puede encontrarse en el RFC 3680.

9) Precondiciones o *Preconditions*: especifica un método de negociación de QoS, seguridad y otros comportamientos de llamada entre dos terminales. Información más detallada puede encontrarse en el RFC 4032.

10) Reserva de recursos IMS: especifica cómo realizar reserva de recursos para llamadas de teléfono o sesiones. Más información en el RFC 3312.

11) SDP o Session Description Protocol: el SDP define el proceso de negociación básica para los flujos de medios e incluye el códec y ancho de banda que hay que usar, así como otros atributos. IMS extiende el SDP con incluso más extensiones tal como la agrupación de flujos, QoS y atributos de precondiciones, soporte de códec suplementarios y modificadores de ancho de banda.

A continuación, ponemos un ejemplo en el que cabe destacar la línea m= a partir de la cual se describe con atributos (a=) la descripción de un componente multimedia:

```
v=0
o=jku2 0 0 IN IP4 213.20.128.35
s=sesión
c=IN IP4 213.20.128.35
b=CT:1000
t=0 0
m=audio 54742 RTP/AVP 97 111 112 6 0 8 4 5 3 101
a=rtpmap:97 red/8000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:6 DVI4/16000
a=rtpmap:0 PCMU/8000
a=rtpmap:4 G723/8000
a=rtpmap: 3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

12) XML: la señalización de SIP IMS usa los protocolos XML, incluyendo XCAP, para implementar varios tipos de contenidos de mensajes SIP y permitir interfaces de funcionalidad completa entre las entidades IMS.

13) Extensiones IMS SIMPLE: el SIMPLE es un grupo de trabajo de IETF que define los requerimientos en señalización de los servicios de presencia y mensajería instantánea. Las definiciones básicas de SIMPLE fueron inadecuadas

para las aplicaciones de IMS porque no eran suficientemente eficientes para usarse en un enlace inalámbrico. SIP IMS extendieron este estándar con lo siguiente: publicaciones y notificaciones parciales; filtrado de notificaciones; y lista de recursos.

3.4.2. Protocolo Diameter

El protocolo Diameter deriva del protocolo RADIUS con muchas mejoras en distintos aspectos, tales como la gestión de errores y fiabilidad de entrega de mensajes. Utiliza la esencia del protocolo AAA de RADIUS y define una serie de mensajes básicos definidos en la recomendación Diameter Base Protocol (RFC3588). Diameter es usado en IMS para intercambio de información relacionada con tareas de AAA (*Authentication, Authorization* y *Accounting*).

Con el Diameter Base Protocol se pueden implementar aplicaciones de gestión de AAA y de hecho IMS lo hace así. Por ejemplo, cuando decimos que un punto de referencia entre un S-CSCF y el HSS es el Cx, significa que la aplicación que se implementa con el protocolo Diameter es precisamente la Cx, el cual incluirá sus propios mensajes de petición-respuesta y los parámetros (llamados *Attribute-Value Pair* o AVP) que los componen. Y así se da con todas las interfaces basadas en Diameter que hemos ido mencionando en este documento.

> Por ejemplo, la interfaz Rx, como aplicación que es, tiene asociado un identificador (*Application ID*) que es único y tiene unos mensajes (o también llamados comandos) bien definidos para acometer su función. Cada mensaje contiene una lista de AVP que definen su contenido. Esta especificación de la aplicación debe estar recogida en un documento, que en el caso del Rx este documento es el 3GPP TS 29 214.

El protocolo Diameter se puede basar en TCP o en SCTP.

Nodos y agentes Diameter

El protocol Diameter está diseñado para arquitecturas *peer-to-peer*. Cada host que implementa el protocolo Diameter puede actuar como cliente o servidor dependiendo del despliegue de la red. Así pues, el término ***nodo*** de Diameter se refiere tanto a un cliente como a un servidor o a un agente de Diameter.

> En un entorno en el que los usuarios establecen conexiones punto a punto con un NAS (servidor de acceso a la red), el NAS es el cliente Diameter con respecto al servidor de autenticación, el cual es el Diameter server. Es decir, que el NAS recibe un mensaje de petición de conexión de usuario y gracias al nodo Diameter que posee el NAS, aglutina la información de credenciales del usuario y se la envía en un mensaje de petición de autenticación al servidor Diameter, que procesa el mensaje. Este servidor envía un mensaje de respuesta con el resultado de la autenticación (ya sea satisfactoria o no) al cliente.

En las transacciones con mensajes Diameter existe, como en SIP, el concepto de dominio, el cual va siempre especificado en todos los mensajes Diameter. Esta información de dominio ayuda a los nodos a procesarlos de un modo u otro.

Hay un tipo especial de nodo de Diameter llamado agente. Hay cuatro tipos de agentes:

- ***Relay agent***: se usa para traspasar un mensaje al destino apropiado dependiendo de la información contenida en el mensaje (dominio de destino).

- ***Proxy agent***: se usa para traspasar mensajes al destino apropiado (aunque sea a otro dominio), pero a diferencia del *Relay Agent*, puede modificar el contenido del mensaje y por lo tanto, proporcionar servicios de valor añadido, aplicar reglas o realizar tareas administrativas en un dominio específico.

- ***Redirect agent***: actúa como un repositorio de configuración centralizado para otros nodos Diameter. Cuando recibe un mensaje, chequea su tabla de rutas y devuelve un mensaje de respuesta junto con información de redirección al nodo que ha enviado la petición. Esto sería muy útil para que un nodo no tenga que almacenar una larga lista de rutas.

- ***Translation agent***: convierte un mensaje de un protocolo AAA a otro (por ejemplo, de Radius a Diameter).

Mensajes Diameter

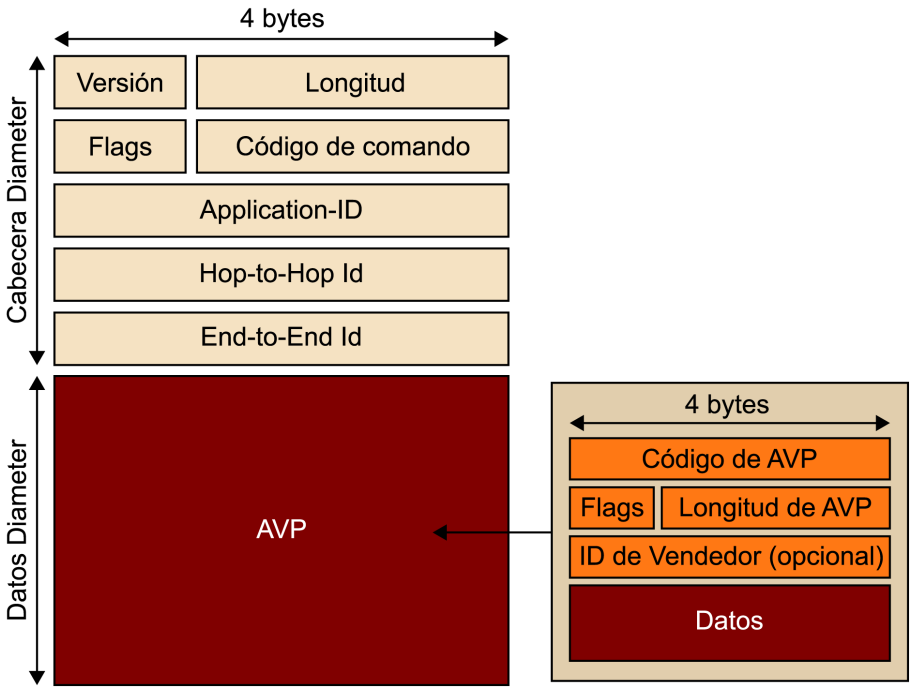
Un mensaje Diameter es la unidad base para enviar un comando o entregar una notificación a otros nodos Diameter. Dependiendo de la aplicación a implementar, el protocolo Diameter ha definido varios tipos de mensajes, que son identificados por su código de comando.

Como el intercambio de mensajes en Diameter es síncrono, cada mensaje tiene su contraparte correspondiente (petición-respuesta), que comparte el mismo código de comando.

Por ejemplo, el Diameter Base Protocol define el CER (*Capability-Exchange-Request*) y CEA (*Capability-Exchange-Answer*) y ambos tienen el mismo código, con la diferencia de un *flag* de request activado o no. Además, el intercambio de CER/CEA debe ser llevado a cabo entre dos nodos Diameter para intercambiar información de aplicaciones soportadas por ambos.

El código de comando indica la intención del mensaje, pero los datos reales que lleva en su interior están contenidos en un grupo de Pares Atributo-Valor o AVP (*Attribute-Value-Pair* en inglés). El protocolo Diameter fija una lista de AVP fijos comunes e impone para cada AVP una semántica correspondiente. Estos AVP llevan los detalles de la información de AAA y encaminamiento, seguridad y capacidades entre dos nodos. Además, cada AVP se asocia con un AVP Data Format que es definido en el Diameter Base Protocol (por ejemplo, OctetString, Integer32), con lo que cada AVP debe seguir el formato de datos concreto. La Figura 13 muestra los campos que componen un mensaje de Diameter.

Figura 13. Campos de mensaje Diameter y AVP.



Cada AVP tiene un código que identifica el tipo de información que contiene. Si existen dos AVP definidos con el mismo código, la manera de diferenciarlos es con el *Vendor ID*, que indica el identificador del fabricante o entidad que ha definido ese AVP (se trata de un identificador asignado por la IANA[2]).

(2)La ETSI o 3GPP tienen su propio identificador de la IANA: 13019 y 10415 respectivamente.

Hay una serie de AVPs que deben existir para facilitar el encaminamiento hacia el nodo destino.

Según la especificación de la aplicación de Diameter a implementar, se pondrá un valor en el campo de *Application-ID*[3] u otro (asignado también por la IANA).

(3)Para la interfaz Rx el *Application-ID* es 16777236.

Entidades de estandarización como 3GPP

Las entidades de estandarización, como el 3GPP, han publicado documentación en la que describen todas las interfaces basadas en Diameter que aparecen en sus especificaciones, donde se les asigna un *Application-ID*. En estos documentos se proponen todos los comandos que forman la interfaz y por cada comando, dependiendo de si es *request* o *answer*, se definirán todos los AVP.

Ejemplo

Por ejemplo, se necesita el AVP *Destination-Host* (código AVP 293) y el *Destination-Realm* (código AVP 283). Estos AVP están definidos en el RFC 3588 como Diameter Base Protocol (con lo cual el *Vendor ID* es 0).

3.5. Ejemplos de flujos de llamadas IMS

Con tal de afianzar los conceptos hasta ahora explicados, vamos a dar dos ejemplos típicos de señalización IMS. En estos ejemplos se ve más clara la interacción entre el núcleo IMS y las entidades de control de admisión y recursos de la subcapa de control de transporte en la garantía de QoS extremo a extremo.

Los tres ejemplos que vamos a ver son los descritos a continuación:

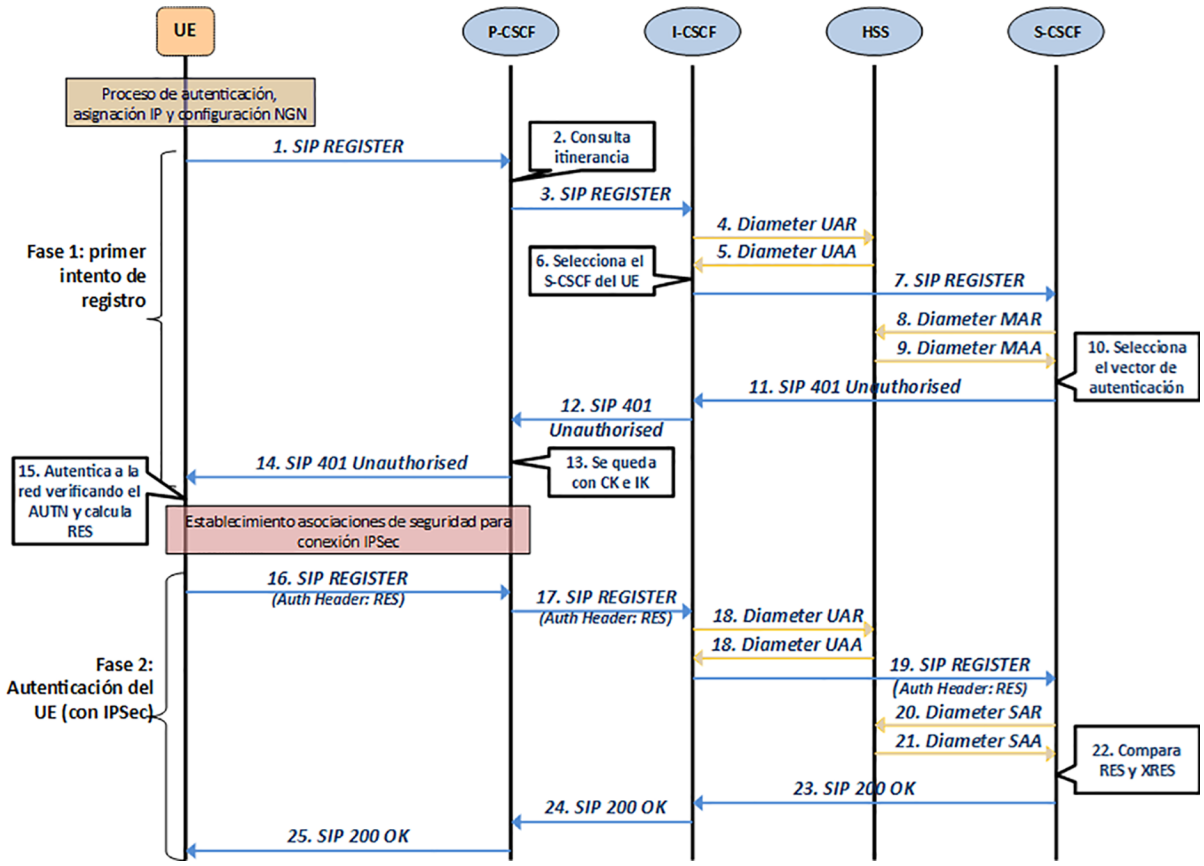
1) Registro en el núcleo IMS.

2) El establecimiento de una llamada de voz a través de dos núcleos IMS para ver la interacción entre dos dominios.
3) Interacción con un servidor de aplicaciones (AS), en este caso con un servicio de presencia en IMS.

3.5.1. Registro en el núcleo IMS

Seguidamente vamos a ver mensaje a mensaje el proceso de registro en el núcleo IMS.

Figura 14. Paso a paso del registro en núcleo IMS.



Paso 1: el UE (cliente IMS) envía un mensaje SIP REGISTER hacia la IP del P-CSCF cuyo *hostname* ha recibido en la fase de adhesión a la red de acceso (por ejemplo, LTE). La IP la descubre vía consulta de DNS. Añade una cabecera *Via:* con su *hostname* para decir que el mensaje ha pasado por él.

Paso 2: el P-CSCF recibe el SIP REGISTER y gracias a la cabecera *Contact:* conoce la dirección IP asignada al UE. También observa en su contenido el dominio del SIP URI del usuario. Esto le indica si el usuario está en itinerancia o no. Si lo está, redirige el mensaje al IBCF (vía interfaz Mw) de su dominio, que le conecta con el dominio destino o con otro dominio que haga de tránsito al dominio de destino. En este ejemplo, no hace itinerancia, con lo cual ha de redirigir el mensaje a un I-CSCF (el P-CSCF no conoce el S-CSCF asociado al UE) descubriendo su dirección IP vía DNS.

Paso 3: el P-CSCF añade al SIP REGISTER algunas cabeceras (por ejemplo, añade al *Via:* su *hostname*, para notificar que el mensaje ha pasado por el).

Paso 4: el I-CSCF recibe el SIP REGISTER y su función es saber a qué S-CSCF de su dominio ha de reenviarlo. Para saberlo envía una petición Diameter con el comando *User Authorization Request* al HSS (vía la interfaz Cx), donde le solicita la lista de S-CSCF.

Paso 5: el HSS contesta con un *User Authorization Answer* incluyendo la lista de S-CSCFs candidatos y sus capacidades.

Paso 6: de la lista recibida desde la interfaz Cx, el I-CSCF selecciona un S-CSCF basado en sus capacidades. También añade una cabecera *Via:* más con su *hostname*.

Paso 7: el I-CSCF reenvía al S-CSCF seleccionando el SIP REGISTER.

Paso 8: el S-CSCF se da cuenta de que el mensaje SIP REGISTER no incluye información de autenticación. Consulta al HSS por la interfaz Cx sobre información para la autenticación del UE usando el comando *Multimedia Authentication Request*.

Paso 9: el HSS responde con un *Multimedia Authentication Answer* incluyendo el *Random number* (RAND), *Authentication token* (AUT), *signed result* (XRES), *Cipher Key* (CK) y *Integrity Key* (IK).

Paso 10: el S-CSCF selecciona el *Authentication vector* (formado por los cinco parámetros anteriores) a usar para autenticar el UE.

Paso 11: el S-CSCF añade el *Authenticacion vector* al mensaje de respuesta al SIP REGISTER de error de autenticación (código 401) incluyendo en la cabecera *www-Authenticate:* los parámetros del *Authentication vector*. El mensaje de respuesta viajará por los mismos nodos que incluya en todas las cabeceras *Via:* recibidas. Con lo cual el mensaje se reenvía al I-CSCF.

Paso 12: el mensaje de respuesta 401 pasa al P-CSCF.

Paso 13: aquí el P-CSCF extrae de la cabecera *www-Authenticate:* el CK y e IK que usará para llevar a cabo las asociaciones de seguridad con UE y establecer una conexión IPSec. Elimina estos dos parámetros de dicha cabecera antes de enviar el mensaje.

Paso 14: envía el mensaje *401 Unauthorized* al UE para retarle en la autenticación.

Paso 15: el UE, usando el *Authentication Token* (AUT) autentica a la red y calcula con sus claves el parámetro RES (que deberá coincidir con el parámetro XRES en poder del S-CSCF). Sus propias claves CK y IK son calculadas con los parámetros recibidos en el *Authentication Vector* (deberían concordar con las que tiene el P-CSCF).

Paso 16: el UE envía el SIP REGISTER de nuevo al P-CSCF, pero esta vez ya cifrado por IPSec e incluyendo el valor calculado RES en la cabecera *Authorization*.

Paso 17: el P-CSCF reenvía de nuevo el mensaje al I-CSCF.

Paso 18: de nuevo el I-CSCF solicita al HSS que le presente la lista de S-CSCFs con un intercambio UAR/UAA.

Paso 19: el I-CSCF reenvía al S-CSCF seleccionado el SIP REGISTER.

Paso 20: solicita al HSS con un comando *Server Assignment Request* información de suscripción del usuario que quiere autenticarse.

Paso 21: el HSS responde con un *Server Assignment Answer*.

Paso 22: compara el valor RES recibido desde el usuario con el valor XRES. Si coinciden, la autenticación del usuario es correcta.

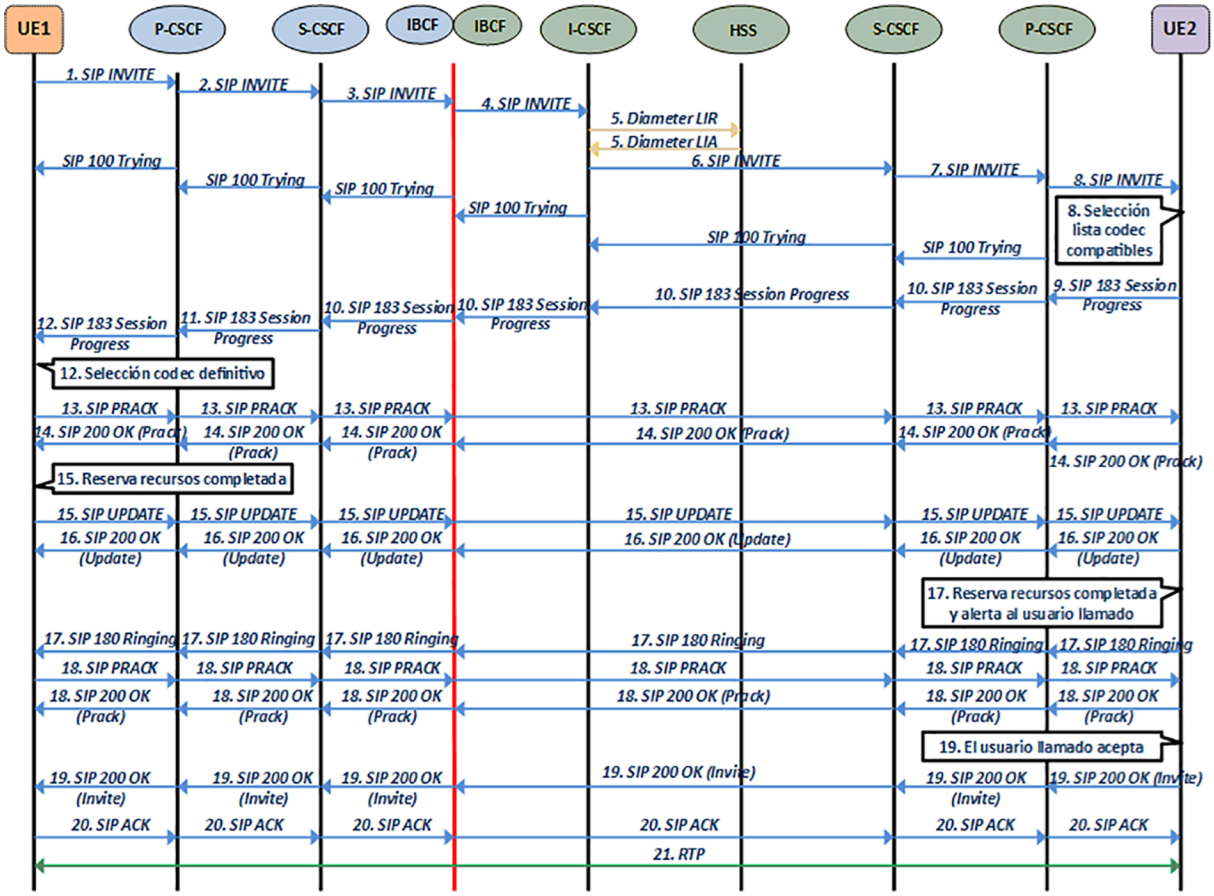
Paso 23 a 25: se envía un mensaje de respuesta de éxito (200 OK) indicando al UE una cabecera de tipo *Service Route:* con el *hostname* del S-CSCF asignado en el registro (lo usará el UE para establecer sesiones de servicio). El P-CSCF aprovechará para registrar al UE como registrado (así como su dirección IP e identidades públicas registradas).

3.5.2. Establecimiento de sesiones de servicio

Seguidamente vamos a ver el ejemplo del establecimiento de una llamada de voz con garantía de QoS extremo a extremo, en el que ambos interlocutores se encuentran en distintos dominios IMS y se ha implementado dicha interconexión con los elementos que el modelo del 3GPP especifica (el IBCF).

La Figura 15 muestra los pasos del flujo de llamada de establecimiento de sesión de voz entre dos clientes SIP: el UE 1 pertenece a un dominio IMS (azul) y el UE 2 pertenece a otro dominio IMS (verde).

Figura 15. Flujo de llamada de voz en IMS.



Paso 1: el UE1 (cliente IMS) inicia una sesión enviando un SIP INVITE hacia el P-CSCF (es decir, con la IP de destino la del P-CSCF) poniendo como objetivo de la llamada la identidad pública del usuario tras el UE 2 (del tipo *SIP URI; usuario2@dominioverde.com*). Añade al mensaje SIP las cabeceras *Contact:* con la dirección IP y el puerto que usa el UE 1 y *Via:* con su *hostname*. También pone dos cabeceras *Route:*. La primera, quizás no tan importante, es para poner el *hostname* del P-CSCF (se pone por si acaso existiera un SIP proxy intermedio entre el P-CSCF y el UE1) y la segunda para indicar a qué S-CSCF debe ir el SIP INVITE (pone el *hostname* que ha obtenido del *200 OK* en la fase de registro). También, y esto es muy importante, se añade una cabecera SDP, donde el UE1 propone unos parámetros de QoS iniciales (*Preconditions*) según los códecs que soporta para voz. Recordemos también que este mensaje se envía a través de la conexión IPSec entre el UE 1 y el P-CSCF, establecida en la fase de registro.

Paso 2: El P-CSCF recibe el SIP INVITE y comprueba una de las cabeceras extendidas para IMS incluidas en el mensaje (*P-Preferred-Identity:*) para que coincida con una de las identidades públicas registradas por el usuario. Luego mira la cabecera *Route:* y extrae el *hostname* del S-CSCF especificado. Lo resuelve vía DNS y reenvía el SIP INVITE a dicho S-CSCF. Antes de enviar el mensaje, el P-CSCF elimina la cabecera *Route:* que llevaba su propio *hostname*, la cabecera *P-Preferred-Identity*: y añade una cabecera *Via:* con su *hostname* para dejar mues-

Notificación envío

En el paso 2, tan pronto como el P-CSCF reenvía el mensaje SIP notifica al elemento adyacente (en este caso al UE) que el mensaje ya se ha tramitado y lo hace con una respuesta del tipo *100 Trying*. Esto se repite para todos los demás elementos que procesan la petición SIP INVITE en el camino.

tra del camino recorrido hasta ahora por el mensaje SIP. También añade una cabecera *Record Route:* para obligar a que, si hay un mensaje de vuelta, este pase por el P-CSCF.

Dominio IMS

Un dominio IMS no tiene por qué tener un IBCF conectado con todos los dominios existentes del mundo. En su lugar, puede tener un IBCF hacia un dominio IMS "en tránsito" al dominio destino. Viene a ser como una especie de ruta por defecto, pero a nivel de dominios IMS destino.

Paso 3: el S-CSCF recibe el mensaje y procede a encaminar el mensaje SIP hacia el dominio destino. Es decir, consulta la parte de dominio de la identidad pública del UE 2 y lo encamina hacia el IBCF, según sus rutas. El S-CSCF elimina la cabecera *Route:* que contiene su propio *hostname*.

Paso 4: el mensaje llega al IBCF del dominio azul, que se encarga de eliminar del mensaje todas las cabeceras que puedan dar pistas a otros dominios sobre la topología del núcleo IMS origen (cabeceras *Via:* sobre todo). El SIP INVITE atraviesa la frontera entre dominios (posiblemente a través de una conexión IPSec entre IBCFs) y llega al IBCF del dominio verde, el cual no sabe en qué S-CSCF está registrado el UE 2. Con lo cual lo reenvía al I-CSCF que tenga configurado para que éste se encargue de él. Añade un *Record Route:* con su *hostname* así como el correspondiente *Via:*.

Funciones de frontera entre dominios

En las versiones del estándar del 3GPP anteriores al *Release 7*, era el S-CSCF del dominio origen (azul en nuestro ejemplo) el que se encargaba de consultar al DNS para conocer la dirección IP del I-CSCF del dominio destino, que era quien hacía las funciones de frontera entre dominios (verde, en nuestro ejemplo) y así reenviar el SIP INVITE directamente. Ahora se han incluido los IBCF para realizar esta función (aportación de la ETSI al estándar del 3GPP).

Paso 5: el I-CSCF del dominio verde consulta al HSS vía la interfaz Cx (Diameter; intercambio de comandos de tipo *Location Information* o LIR/LIA) a qué S-CSCF (*hostname*) hay que enviar el SIP INVITE. Es por ello por lo que añade la cabecera *Route:* con el *hostname* del S-CSCF destino. También puede conocer la dirección IP de destino mediante una consulta DNS y así poder reenviar el mensaje a su destino.

Paso 6: el S-CSCF del dominio verde lee la identidad pública del UE 2 especificada por el UE 1 en el mensaje y comprueba que se encuentra registrado. Si lo está, mapea esta identidad con la dirección IP y el puerto con el que el UE 2 está registrado y la sustituye en el mensaje. Sin embargo, a pesar de tener la IP del usuario final, el mensaje se envía hacia el P-CSCF correspondiente (añadiendo la correspondiente cabecera *Route:*). El S-CSCF añade el *Via:* y un *Record Route:* con su propio *hostname*.

Paso 7: el P-CSCF del dominio verde recibe el mensaje y pueden suceder dos cosas dependiendo de los mecanismos de reserva de recursos de la red donde UE 2 está conectado: en modo *pull* el P-CSCF solicitaría al PCRF (en caso de una red de acceso LTE) un *Authorization token* para incluirlo en el mensaje a enviar al UE 2. En modo *push* el P-CSCF no solicita nada al PCRF porque solo tiene la información de QoS del UE y reenvía el mensaje al UE 2. En ambos casos, antes de enviar el mensaje (a través de la conexión IPSec correspondiente) el P-CSCF incluye en la cabecera *Via:* su *hostname*.

Paso 8: el UE 2 recibe el SIP INVITE con la propuesta de códec del UE 1. Entonces el UE 2 selecciona de esa lista aquellos códec compatibles con los soportados por él y elabora una nueva cabecera SDP con dichos parámetros y actualiza los parámetros de establecimiento de conexión RTP restantes (IP y puertos). Esta nueva cabecera SDP con los parámetros preliminares acordados entre el

UE 1 y el UE 2 se incluye en un mensaje de respuesta provisional de tipo *183 Session Progress*. Las cabeceras *Via:* y el *Record Route:* son copiadas del mensaje SIP INVITE recibido. La cabecera *Contact:* se cambia con la IP y puerto usadas por el UE 2. Se indica también en el mensaje SIP la cabecera *Require:100rel*, con la que le indica al UE 1 que esta respuesta provisional que le envía el UE 2 debe ser respondida con un mensaje PRACK para así saber si el *183 Session Progress* se ha recibido.

Paso 9: la respuesta *183 Session Progress* llega al P-CSCF el cual, si la reserva de recursos es en modo *push*, podría iniciar una primera reserva de recursos antes de reenviar el mensaje de respuesta (hasta que no recibe la respuesta desde el PCRF no reenvía el mensaje SIP).

Paso 10: esta respuesta sigue el mismo camino nodo a nodo que ha trazado el SIP INVITE, pero a la inversa gracias a la cabecera *Via:*. En cada nodo que recala, se elimina el *hostname* correspondiente del *Via:* pero el *Record Route:* no se modifica.

Record Route: y Via:

Fijaos que las cabeceras *Record Route:* y el *Via*: se procesan de manera distinta dependiendo de si el mensaje es una petición o una respuesta.

Paso 11: la respuesta *183 Session Progress*, con una cabecera SDP con una lista de parámetros de QoS pre-negociados entre el UE 1 y el UE 2, llega al P-CSCF del dominio azul. Es en este punto donde el P-CSCF extrae la información de reserva de recursos para enviarla al PCRF vía la interfaz Rx (si se usa modo *push*). En caso de usarse el modo *pull*, P-CSCF solicitaría al PCRF un *Authorization token* para incluirlo en la respuesta a enviar al UE 1. En ambos casos el mensaje de respuesta no se reenvía al UE 1 hasta que el P-CSCF no recibe respuesta a la solicitud realizada.

Paso 12: el UE 1 selecciona los códecs definitivos de la lista recibida en el SDP para usar en la conversación de voz. Como además ve en el mensaje de respuesta que existe la cabecera *Require:100rel*, prepara un mensaje PRACK para el UE 2. Ahora ya tiene el códec definitivo, y dependiendo del modelo de reserva de recursos de la red de acceso del UE 1 realizará una acción u otra. Si es modo *pull* el UE 1 inicia los mecanismos propios que tenga la red de acceso para garantizar la QoS negociada (en una red LTE se solicitaría el establecimiento de un túnel EPS dedicado). En dicha petición de recursos el UE 1 debe incluir el *Authorization Token*, si existe. Si es modo *push*, el UE1 no hará nada puesto que el establecimiento del túnel dedicado ya se habría iniciado en el anterior paso.

Paso 13: el PRACK recorre todo el camino hasta el UE 2 del dominio verde, el cual realiza las siguientes acciones dependiendo del modelo de reserva de recursos: si es en modo *pull* se solicitaría desde el UE el establecimiento del túnel EPS dedicado. Si es modo *push*, el UE 2 no hará nada puesto que el establecimiento del túnel dedicado ya se habría iniciado desde el PCRF.

Paso 14: la respuesta al PRACK (200 OK) recorre todo el camino de vuelta hasta el UE 1. Sin embargo, al pasar por los P-CSCF respectivos de los dominios azul y verde, pueden realizar sendas actualizaciones de la reserva de recursos con la información SDP del mensaje de respuesta (esto solo se da si ambos están en modo *push*).

Paso 15: el UE 1 recibe el 200 OK en respuesta al PRACK enviado anteriormente y se prepara para enviar el mensaje de UPDATE con el que notificará al UE 2 sobre el estado definitivo de la reserva de recursos en su red de acceso. Esto se hace enviando dentro del mensaje UPDATE la cabecera SDP con el mismo formato que el PRACK, pero incluyendo el atributo *a=curr: qos local sendrecv*.

Paso 16: el mensaje UPDATE viaja hasta el UE 2. Éste se dará cuenta de que los recursos ya están disponibles en el otro extremo de la llamada y responderá con un 200 OK a dicho mensaje. El 200 OK en respuesta al UPDATE viaja hasta el UE 1 para notificarle la recepción de éste.

Paso 17: el UE 2, como resultado del final del proceso de reserva de recursos en su red de acceso, envía un *180 Ringing* (con la cabecera *Require: 100rel* requiriendo confirmación de recepción al UE 1) para notificar que el UE 2 está alertando al usuario llamado de que se requiere una acción suya para aceptar o rechazar la llamada entrante. El *180 Ringing* (sin información de SDP) viaja hasta el UE 1.

Nota

Fijaos que, si el usuario llamado acepta la llamada, los recursos ya estarían asignados y se podría proceder al envío de flujos de voz RTP sin más dilación. Si la rechaza, provocaría el envío de una respuesta SIP 603 Decline hacia el UE 1, que provocaría la liberación inmediata de todos los recursos reservados en ambas redes de acceso.

Paso 18: se produce un nuevo intercambio de SIP PRACK y 200 OK (pero esta vez sin cabecera SDP). A partir de aquí, el usuario llamante estará a la espera de que el usuario destino decida aceptar o rechazar la llamada.

Paso 19: el usuario llamado (UE 2) decide aceptar la llamada provocando que se envíe un 200 OK, pero esta vez será la respuesta definitiva al primer SIP INVITE enviado por el UE 1.

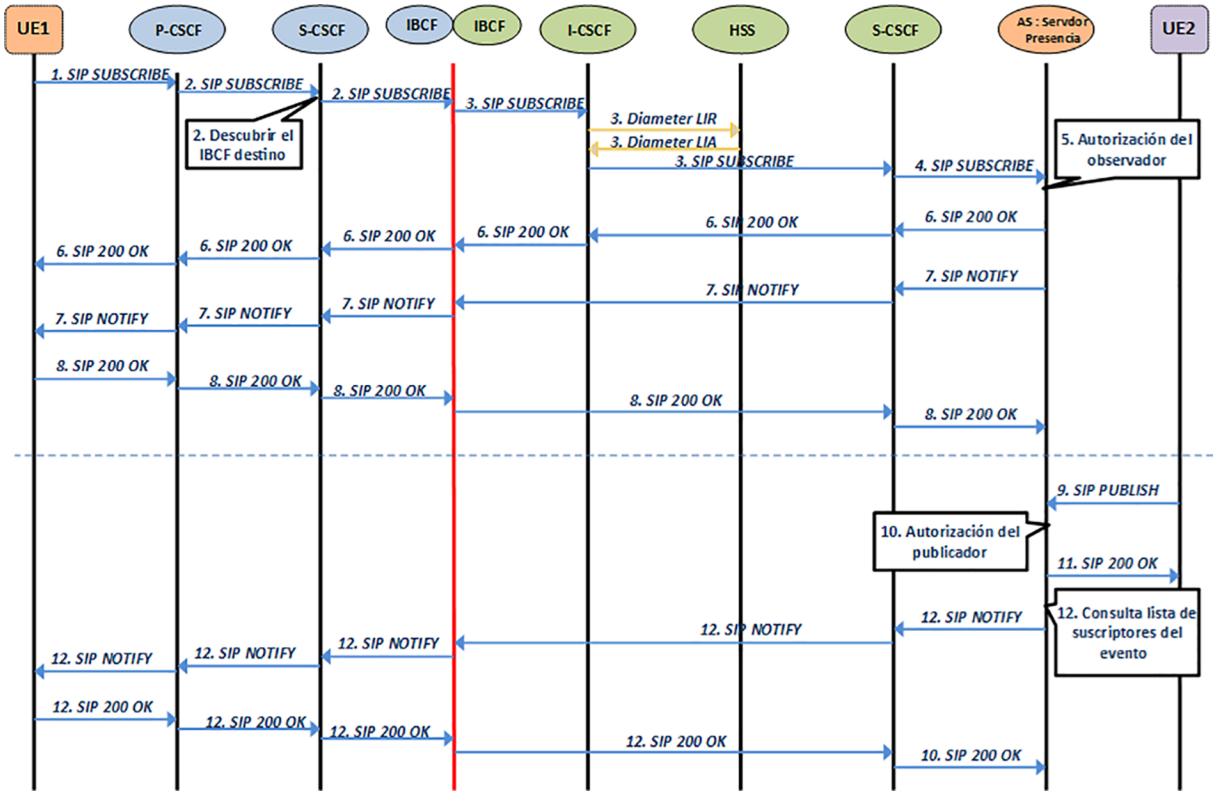
Paso 20: el UE 1 contesta con un SIP ACK final confirmando la recepción del 200 OK.

Paso 21: Llegado a este punto, tanto el UE 1 como el UE 2 ya pueden intercambiar los flujos RTP.

3.5.3. Servicio de presencia

El servicio de presencia es uno de los más importantes que se ofrecen en IMS, ya que es usado por otras muchas aplicaciones y servicios. Veamos, a partir de la Figura 16, paso a paso los mensajes involucrados en este servicio.

Figura 16. Flujo de mensajes SIP en servicio de presencia.



Paso 1: el UE envía un mensaje SIP SUBSCRIBE en el que incluye en la cabecera SIP el campo *Event:* indicando el evento al cual se quiere suscribir. En este caso se trata del evento *presence* (*Event: presence*). El UE indica su propio URI en la cabecera *From:* y la ruta a seguir (*Route:*) para el mensaje SIP indicando el P-CSCF y S-CSCF asignados.

Paso 2: el mensaje SIP SUBSCRIBE pasa por el P-CSCF, que lo hace llegar al S-CSCF asignado al UE dentro del dominio. Ésta consulta el SIP URI de destino (hacia el AS que proporciona el servicio de presencia) que le indicará a qué IBCF (del dominio destino) debe reenviar el SIP SUBSCRIBE.

Paso 3: el mensaje llega finalmente al I-CSCF del dominio que alberga el AS y éste le solicita al HSS (intercambio de mensajes Diameter LIR/LIA) el *hostname* del S-CSCF asignado a tal AS.

Paso 4: el S-CSCF reenvía el mensaje SUBSCRIBE al AS correspondiente.

Paso 5: el AS de presencia autoriza al UE que quiere suscribirse al evento (obtiene el URI del campo *From:*). En caso de autorizarle, éste contesta con un 200 OK.

Paso 6: el 200 OK llega al UE siguiendo el mismo camino de vuelta que el SUBSCRIBE.

Paso 7: en el momento en que se da el evento al cual el usuario se ha suscrito, el AS envía un mensaje SIP NOTIFY hacia el UE con el estado actual de presencia. Este mensaje sigue el mismo camino que el 200 OK exceptuando el I-CSCF.

Paso 8: el UE responde con un 200 OK a dicho NOTIFY.

En el caso de que un usuario modifique su información de presencia, primero se publica en el AS de presencia su nuevo estado y este AS notifica sobre el cambio a todos los UE suscritos a tal evento. Seguidamente lo explicamos paso a paso con un ejemplo:

Paso 9: un UE externo cambia su información de presencia a 'No Disponible'. Entonces éste envía un mensaje SIP PUBLISH hacia el AS con la nueva información de presencia. En el mensaje se incluye la ruta a seguir con la cabecera *Route:* hasta el S-CSCF del dominio de presencia (como cualquier otro mensaje SIP visto hasta ahora).

Paso 10: el AS recibe el mensaje y autoriza al usuario que quiere publicar dicha información sobre él mismo para asegurarse de que puede publicarla.

Paso 11: el AS de presencia contesta con un 200 OK a dicha publicación si el usuario ha sido autorizado.

Paso 12: entonces el AS genera el NOTIFY correspondiente con la nueva información de estado de presencia hacia los UE que se hayan suscrito a dicho evento (igual que en los pasos 7 y 8).

4. Capa de aplicación

En esta sección abordaremos cómo se proveen y se implementan los servicios en las redes NGN usando IMS como capa de control de servicio como base.

4.1. ¿Qué es un servicio en un contexto NGN?

Ante todo, empezaremos por saber qué entendemos por servicio. Estrictamente hablando, y sin meternos en el mundo de las telecomunicaciones ni las tecnologías de la información (IT), **un servicio se puede definir en términos de negocio como cualquier acción o actividad que tiene un valor añadido para un consumidor**, el cual puede ser tanto una persona como un sistema. Esta acción o actividad es ofrecida por un **proveedor de servicio**, que puede ser otra persona, entidad o sistema, el cual obtiene un beneficio al proporcionar dicha acción.

Los servicios en el mundo de las telecomunicaciones que se ofrecían hasta hoy estaban implementados de forma vertical en el sentido de que cada uno disponía de su propio sistema de gestión y operación dedicados. Eran servicios monolíticos e incompatibles entre sí.

Las redes NGN dan un giro a este concepto de servicios, ofreciendo servicios que no solo son **independientes de la tecnología de la red de transporte**, sino que **se descomponen en elementos reutilizables denominados componentes de servicios o también habilitadores de servicios *(service enablers*)**.

Como piezas de un puzle, unos servicios pueden complementarse e integrarse con otros con el único fin de producir un nuevo servicio de valor añadido y de algún modo enmascarar la complejidad de dicha integración al usuario final.

Esta filosofía encaja perfectamente con el concepto de las redes 5G en las que la virtualización de redes y en concreto el NFV-MANO (*Network Function Virtualization Management and Orchestration*) son los conceptos más característicos. Ésta impulsa la híper-fragmentación de funciones y/o servicios en microservicios completamente independientes entre sí y que se ejecutan en entornos virtualizados.

Microservicios

El concepto de "microservicios" también se extiende a los componentes del núcleo IMS en el que sus entidades funcionales (P-CSCF, I-CSCF, etc.) se consideran en sí un servicio que es consumido por otras entidades.

Para poder lograr dicha **integración de componentes de servicios** en otros servicios más complejos, dichos componentes **deben cumplir con las siguientes características**:

- Deben estar bien definidos y diferenciados.
- Deben ser autocontenidos, es decir, que siempre proporcionen la misma funcionalidad independientemente de los otros servicios.
- No deben depender del contexto o estado de otros componentes o servicios.

La integración de servicios también conlleva la definición de interfaces estandarizados que posibiliten la integración de estos componentes. Es esta modularidad e interactividad entre componentes la que posibilita la fácil creación de nuevos servicios futuros, y esto es una de las claves de las redes NGN.

Ejemplos de estos componentes son el servicio de presencia, el de gestión de grupos, mensajería instantánea, etc. Dichos servicios, además, pueden ser provistos por terceros.

De cara a conseguir la independencia entre servicios y tecnología de transporte y posibilitar que terceros (desarrolladores de aplicaciones) puedan desarrollar rápidamente nuevos servicios, se utilizan APIs (*Application Programming Interface*) abiertas.

La industria ha dado a luz a varias API abiertas para el desarrollo de servicios como OSA/Parlay API, JAIN SIP, JAIN SLEE, SIP Servlet y sobretodo APIs basadas en HTTP REST.

En resumen, este nuevo enfoque viene definido por un nuevo paradigma en el mundo de los servicios llamado SOA o *Service Oriented Architecture*, el cual vamos a describir a continuación.

4.2. Introducción al paradigma SOA

El **paradigma SOA** (*Service Oriented Architecture*) es un estilo arquitectural cuyo objetivo es conseguir el desacoplo entre los componentes de *software* que interactúan entre sí. El comportamiento de dichos componentes es definido completamente por APIs e interfaces contractuales, públicos y neutrales, tanto en tecnología como en plataforma.

Los principales objetivos de SOA en comparación con otras arquitecturas *software* usadas en el pasado radican en la obtención de lo siguiente:

- Una mayor rapidez de adaptación del *software* a las necesidades comerciales cambiantes.
- Una reducción del coste de integración de nuevos servicios, así como del mantenimiento de servicios ya existentes.

SOA reorganiza las aplicaciones de *software* existentes y los componentes en un set de servicios autocontenidos y autodefinidos, definiendo interfaces estándares y protocolos de mensajería entre estos *software*. Estos servicios pueden ser accedidos sin que sea necesaria una conectividad punto a punto tradicional, basada en diferentes protocolos. Cualquier servicio SOA puede asumir el rol de cliente o de servidor con respecto a otro servicio, en función de la situación.

Un ejemplo en la que la arquitectura SOA se ha implantado y se está usando de manera extensiva es en *cloud computing*. Amazon lo implementa en su *Amazon Web Services* para sus servicios web. Permite a los usuarios construir sus propias aplicaciones web de manera escalable usando cada uno de los componentes de servicios que Amazon ofrece como un bloque estable y fácil de utilizar. Dichos bloques pueden ser usados por separado o enlazados con otros servicios de AWS utilizando comunicaciones específicas y bien definidas.

El paradigma SOA permite que procesos y transacciones de negocio complejos puedan ser proporcionados como servicios integrados permitiendo a las aplicaciones ser reutilizadas en cualquier lugar y por cualquiera.

Arquitectura SOA

Debéis tener en cuenta que SOA no es una tecnología, sino un modelo arquitectural de *software* distribuido. Sin embargo, existen tecnologías para crear *software* con arquitectura SOA, como por ejemplo BPEL de Oracle o opciones de código abierto como Mule Studio de Mulesoft.

Un SOA básico incluye tres procedimientos fundamentales:

- **Provisión de servicio:** los proveedores desarrollan aplicaciones que proporcionan servicios a los clientes. En la provisión de servicio se incluye también un plan de tarifas (si las hubiera) o la definición incluso de aspectos de seguridad y disponibilidad para el usuario.

- **Registro de servicio:** es un directorio llamado *Universal Description Discovery and Integration* (UDDI), en el que los proveedores de servicio pueden registrar información sobre los servicios que ellos ofrecen y donde clientes potenciales pueden descubrirlos y buscarlos.

- **Cliente de servicio:** es la herramienta que utiliza el consumidor del servicio. Este último no es consciente de la complejidad de los servicios ni tampoco de su descomposición en componentes. Todo lo que sabe y por lo que se preocupa es por su acuerdo con el proveedor de servicios o SLA (*Service Level Agreement*), y por las aplicaciones instaladas o el equipo utilizado para poder disponer del servicio.

Junto con estos procedimientos, SOA también define tres funciones importantes:

- **Publicación del servicio:** el proveedor publica en el registro de servicio información descriptiva sobre su servicio, para que el cliente pueda saber qué capacidades tiene y cómo acceder a él.

- **Descubrimiento de servicio:** El cliente recurre al registro para conocer de una manera sencilla e inteligible todos los servicios disponibles.

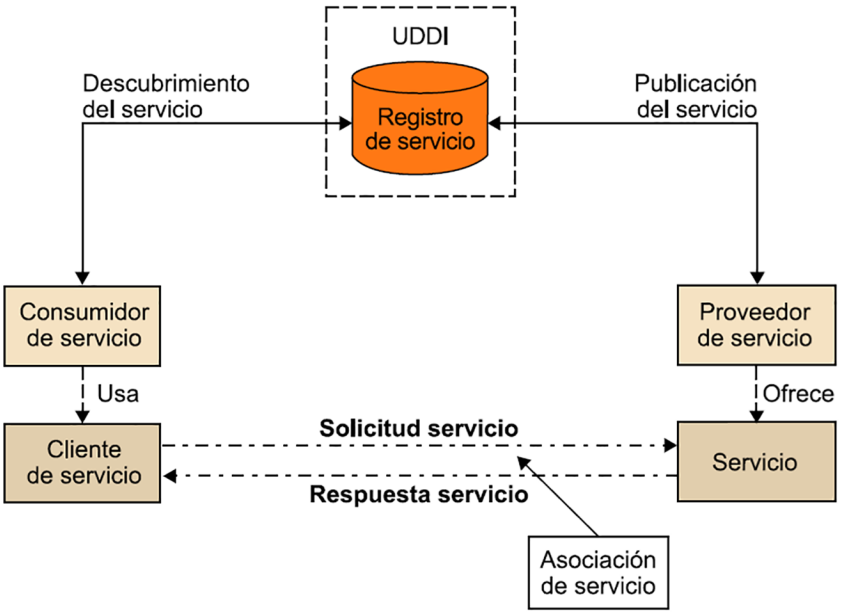
- **Asociación al servicio:** una vez un cliente quiere invocar un servicio a un proveedor concreto, realiza una solicitud (a través de la interfaz correspondiente) dirigida a éste, el cual envía una respuesta acorde a dicha solicitud (provisión del servicio).

SOA define una interacción entre los clientes de servicio y los proveedores de servicio, estos últimos son responsables de publicar una descripción de los servicios en el UDDI (ver la Figura 17). Para publicar dicha descripción de los servicios (interfaces de servicios web, en este caso) el UDDI se sirve del lenguaje WSDL (*Web Services Description Language*).

Como ejemplo de UDDI, tenemos el caso típico del servicio de reserva de billetes de avión por Internet. No solo se puede realizar por la misma web de la aerolínea, sino por infinidad de buscadores web de billetes de avión y/o hoteles. Las aerolíneas pueden registrar sus servicios de reserva de vuelos en un directorio de UDDI, las agencias de viajes pueden buscar las interfaces o los contratos de los servicios web de las aerolíneas, y una vez encuentren el que necesitan, puede empezar a usarlo inmediatamente.

La publicación, no solo de los servicios sino de los componentes reutilizables de telecomunicación (llamados habilitadores de servicios o *service enablers*), permite la construcción de aplicaciones con su lógica de servicio específica y el uso de estos habilitadores. Esta reutilización permite reducir los costes de introducción de servicios múltiples, siendo una de las principales ventajas finales de basarse en SOA.

Figura 17. Arquitectura SOA.



Importancia de la orquestación de los servicios en SOA

Sabiendo que un servicio puede estar formado por varios componentes de servicios, parece obvio que se deba desarrollar alguna tarea de mediación u orquestación que proporcione coordinación en el uso de los componentes.

Los componentes de los servicios se alojan en una o más plataformas de suministro de servicio llamadas SDP o *Service Delivery Platforms*. Estas plataformas ofrecen un marco para la fácil creación, orquestación y ejecución de servicios, así como la gestión de aplicaciones provenientes de terceros. La integración del SDP con las funciones de red es única (la misma interfaz con la red es utilizada por todos los servicios).

Mediante orquestación, las capacidades de los diferentes SDP se pueden combinar para crear nuevos servicios reutilizando sus capacidades. De esta manera se reducen los esfuerzos y los costes en el desarrollo de servicios y el tiempo de lanzamiento de estos al mercado.

Si tuviéramos más de un SDP a integrar entre sí, las interacciones entre estos se extraerían hacia una capa externa de orquestación, lo cual reduce las dependencias e incrementa la flexibilidad de los servicios en un entorno de múltiples proveedores.

La capa de orquestación no solo toma el rol de la integración de la ejecución y de la orientación de la gestión, sino que, además, lo que es más importante, juega un papel esencial en la definición e implementación de la gestión y de la ejecución de la lógica del servicio.

¿Cómo se comunican los servicios entre sí y qué recomienda la industria para implementar SOA a nivel de protocolos?

En el contexto de implementación de servicios donde hay bloques de *software* independientes que interaccionan para formar un servicio más complejo es normal pensar en un esquema consumidor-productor. Es decir, un consumidor (que puede ser un componente de *software* o directamente un usuario) consume unos servicios o recursos que otro bloque produce (esta arquitectura es algo muy típico en servicios web). Y es en este contexto donde se utilizan protocolos que se adaptan a este intercambio de información.

Existen principalmente dos tecnologías para implementar servicios que cumplan SOA: SOAP y REST. Aunque SOAP es unos de los protocolos más usados para implementar SOA, la tecnología REST está extendiéndose cada vez más. La principal diferencia entre SOAP y REST es la filosofía que siguen para realizar invocaciones remotas.

REST

En inglés significa *Representational State Transfer.*

SOAP

En inglés significa *Simple Object Access Protocol.*

REST sigue un método basado en el acceso a recursos vía interacciones basadas en web. Con REST, se localiza un recurso en un servidor y se elige actualizar dicho recurso, borrarlo o conseguir alguna información sobre el.

Con SOAP, el cliente no elige interactuar directamente con un recurso, pero en lugar de ello llama a un servicio. Este servicio mitiga el acceso a varios objetos y recursos que hay detrás.

SOAP ha construido un gran número de entornos y APIs sobre HTTP, incluyendo el WSDL (*Web Services Description Language*), el cual define la estructura de datos que se intercambian entre un cliente y un servidor.

SOAP (*Simple Object Access Protocol*) define una especificación o grupo de reglas de un protocolo estándar de comunicación en el que se intercambian mensajes basados en XML. A nivel de protocolos de transporte soporta HTTP y SMTP. El estándar HTTP se adapta mejor ya que puede traspasar cortafuegos y *proxies* sin ningún impacto en el protocolo SOAP.

REST (*Representational State Transfer*) no es un protocolo propiamente dicho, sino que describe un grupo de principios arquitecturales por los cuales los datos pueden ser transmitidos sobre una interfaz estandarizada (tal como HTTP). REST no especifica una estructura de mensajería propia y solo se focaliza en el diseño de reglas para crear servicios sin estado. Consecuentemente, un ingeniero de *software* dispone de libertad para diseñar la estructura de la información contenida en el cuerpo de los mensajes intercambiados. Un cliente REST puede acceder a un recurso usando el URI único y una representación del recurso es retornado. Cuando se accede a los recursos con el protocolo HTTP, el URL del recurso sirve como un identificador del recurso y las operaciones estándar de HTTP (como GET, PUT, DELETE, POST y HEAD) representan las operaciones que se realizan sobre dicho recurso. La información intercambiada en el cuerpo de los mensajes HTTP suele ser codificada usando JSON o XML.

URI

En inglés significa *Unique Resource Identifier* y en HTTP REST es un URL como si se accediera a una página web con múltiples carpetas, cada una de ellas alberga un recurso.

4.3. Integración de los servicios NGN en el paradigma SOA

En este apartado nos adentramos en el campo de la integración de los servicios de comunicaciones multimedia (basados en SOA) en un entorno NGN en el que existe el núcleo IMS como subsistema de control de sesión de servicio.

A continuación, describiremos el Servidor de Aplicación o AS como entidad más representativa en la provisión de servicios en NGN/IMS.

Servidores de aplicaciones

Los **servidores de aplicaciones (*Application Servers*, AS)** son el elemento central de la arquitectura de servicios de NGN/IMS. Su función es la de albergar y ejecutar los servicios de valor añadido de la plataforma, así como comunicarse con el Núcleo IMS (singularmente con el S-CSCF) haciendo uso del protocolo SIP. Los servidores de aplicaciones no son estrictamente entidades de IMS, sino más bien funciones que se construyen para interactuar con el núcleo IMS a un nivel superior. No obstante, en ellos recae la provisión de la mayoría de los servicios que aportan valor a IMS.

Los atributos fundamentales de un servidor de aplicaciones son:

- Posibilidad de recibir y procesar una sesión SIP entrante procedente de IMS.
- Capacidad para realizar peticiones SIP.
- Capacidad para enviar información a las funciones de facturación.

Los servidores de aplicaciones pueden operar como tres tipos distintos de entidades SIP: como agente de usuario (UA), como proxy y como agente de usuario inverso (B2BUA o *Back-to-Back User Agent*). Éstos servidores pueden estar situados dentro de la red local a la que está conectado el usuario o bien operar independientemente desde una red externa. Por otra parte, un AS puede estar dedicado a proporcionar un único servicio mientras que un usuario puede utilizar más de un servicio simultáneamente, por lo que un mismo suscriptor puede hacer uso de uno o más servidores de aplicaciones e incluso puede haber sesiones en las que intervenga más de un AS.

SIP, UA y B2BUA

En SIP, *user agent* o agente de usuario (UA) representa uno de los extremos de la comunicación SIP (por ejemplo, en un cliente SIP se ejecuta un UA de SIP). Sin embargo, un proxy SIP, al no ser el destinatario final de un mensaje SIP, su función es reenviarlo a otro proxy o al UA destino. Finalmente, un B2BUA son dos agentes de usuario en la misma máquina, pero interconectados entre sí por algún tipo de lógica o funcionalidad. En este último caso dos sesiones SIP totalmente independientes se interconectan mediante dicha lógica.

En la Figura 18 podemos ver cómo la capa de control de servicio (representado por el núcleo IMS) se interconecta con el servidor de aplicación (AS) por una interfaz SIP (según el 3GPP se llama ISC[4] o IMS Service Control) y ésta con la aplicación en sí a través de una API de programación abierta. Es precisamente esta API la que representa la interfaz ANI del modelo de referencia de la ITU-T de NGN (Figura 1).

(4)En algunas partes a la interfaz ISC se la llama también SIP+.

Vemos también en dicha figura que el S-CSCF no es el único elemento del núcleo IMS interconectado con el AS. El I-CSCF también tiene una interfaz dedicada de interconexión llamada Ma y que está basada en SIP, como la interfaz ISC. Esta interfaz permite que el I-CSCF reciba una petición SIP entrante dirigida a un PSI (*Public Service Identity*) que la resuelve a un AS particular. El I-

CSCF encamina la petición directamente al AS vía la interfaz Ma. Esta interfaz también es usada por el AS cuando necesita iniciar una sesión hacia un usuario o PSI y este AS no tiene conocimiento previo sobre a qué S-CSCF está asociado dicho usuario o PSI.

A pesar de que el I-CSCF tiene esta funcionalidad de interacción con los AS, a partir de ahora nos centraremos exclusivamente en el uso de la interfaz ISC, ya que es el caso más común.

Volviendo a la Figura 18, podemos ver también que tanto el AS como los CSCF del núcleo IMS tienen acceso al HSS por sendas interfaces basadas en Diameter Sh y Cx respectivamente. Dichas interfaces son utilizadas por estas entidades para descargar información de suscripción relacionada con las aplicaciones (*Service Profile*) que el usuario tiene permitido acceder. En esta información de suscripción se encuentra el iFC o *initial Filter Criteria*.

El **iFC o *initial Filter Criteria*** (3GPP TS 23.218) es una lista de parámetros que componen el *Service Profile* y forman parte de la información de suscripción del usuario que ayuda al S-CSCF a decidir a qué AS se tiene que enviar una petición SIP determinada (que puede ser un REGISTER, INVITE, SUBSCRIBE, NOTIFY o MESSAGE). Esta información, que tiene carácter estático, la recibe el S-CSCF desde el HSS vía la interfaz Cx en forma de *Trigger Points*. Un iFC está formado por los siguientes parámetros:

- ***Priority level*:** nivel de prioridad sobre el cual se debe aplicar un iFC con respecto a otros iFCs en el mismo *Service Profile*. Éste parámetro viene a indicar el orden en el que se aplican (cuanto más bajo el número más prioritario es, sin necesidad de que sean números consecutivos)

- ***Trigger Points*:** está compuesto por un conjunto de *Service Point Triggers* (que se describen más adelante).

- ***Application Server*:** se especifican los datos que definen el SIP AS al cual hay que enviar el mensaje SIP. Estos datos son:
  - SIP URI: alias (resoluble vía DNS) que identifica el SIP AS de manera única (puede ser una dirección IP directamente).

  - Default Handling: define la acción a realizar (abortar o continuar la sesión) si el *Service Broker* (que veremos más adelante) o el S-CSCF no puede establecer conexión con el AS, sea cual sea el motivo.

Priority level

Tenéis un ejemplo de cómo se aplica el *priority level* y los *trigger points* en la orquestación de componentes de servicio en el final de la sección 4.4.2.

– Service Information: datos adicionales que el AS puede requerir para procesar la solicitud.

Los *Trigger Points* están formados por un conjunto de comparaciones de campos del mensaje SIP que, como ya se ha comentado antes, se llaman *Service Point Triggers*. La interrelación entre estos SPT en un *Trigger Point* se define según otro parámetro llamado *Condition Type CNF* que puede tener dos valores:

- ***Disjunctive Normal Format*:** en el que los SPTs se aplican en ANDs anidados entre ORs.
  (SPT1 **AND** SPT2 **AND**…) **OR** (SPTn **AND** SPTm **AND**...) **OR** (...).

- ***Conjunctive Normal Format*:** en el que los SPTs se aplican en ORs anidados entre ANDs.
  (SPT1 **OR** SPT2 **OR**…) **AND** (SPTn **OR** SPTm **OR** …) **AND** (...).

Dentro de un anidado de ANDs o de ORs se puede dar el caso de tener solo un SPT (ver ejemplo para *Disjunctive Normal Format* a continuación).

(SPT1) **OR** (SPTn **AND** SPTm **AND**...) **OR** (SPT2)

Cada SPT se define por los siguientes campos para fijar las condiciones para hacer un match en el mismo:

- **Negación o "Not":** Hará *match* siempre y cuando no se cumplan las condiciones que se indican en el SPT. Este campo se considera como un *checkbox*: "activado" [X] o "no activado" [ ].

- **Tipo de campo:** Indica el tipo de información a consultar. Normalmente es uno entre los siguientes valores por cada SPT: *RequestURI*, *SIP Method*, *SIP Header, Session Case* o SDP line.

a) **Valor de campo:** Dependiendo del tipo de campo que se haya seleccionado el contenido puede cambiar. A continuación, se lista el tipo de contenido que se espera según cada tipo de campo:
   – **Request URI**: texto o parte del texto a comparar en este campo del mensaje SIP. Normalmente se utiliza notación de *Regular Expression* (o también llamado Regex).

   Ejemplo que expresa un Request URI cualquiera que vaya al dominio home-domain.net: "sip: *@home-domain.net".

   – **SIP Method**: indica el mensaje SIP a comparar (INVITE, REGISTER, SUBSCRIBE, ...).

   – **SIP Header** indica primero, la cabecera dentro del mensaje y luego su contenido con notación Regex (*regular expression*).

Ejemplo que expresa un SIP Header "From" cualquiera con dominio home-domain.net: header type: "From:" header value: "*@home-domain.net".

- **Session Case**: indica la dirección del mensaje SIP, de la cual hay dos tipos principales:
  - "*UE-originating*": perfil para peticiones SIP salientes (generadas por el usuario suscriptor).
  - "*UE-terminating*": perfil para peticiones SIP provenientes de otro usuario y que van hacia el usuario suscriptor en cuestión.

- **SDP line**: en este caso, solo aplica a líneas que se usan en la negociación de códecs, que es de tipo SDP (*Session Description Protocol*). Se indica primero, el tipo de línea SDP (m, a, c, etc.) y luego su contenido con notación Regex.

Ejemplo que expresa que exista en SDP un componente de multimedia de video cualquiera: *SDP line: "m" SDP line value: "*video**".

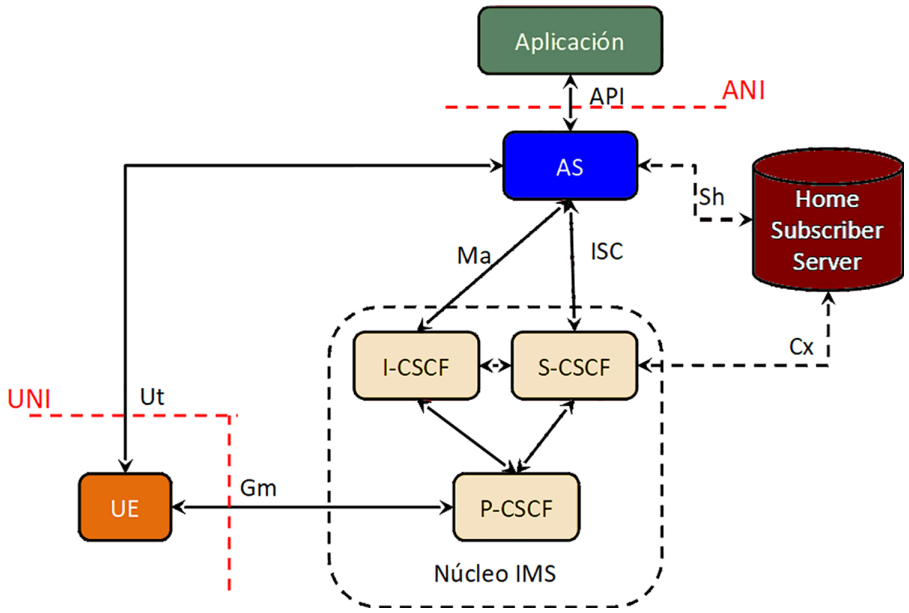
Precisamente, con respecto al usuario (representado como UE en la Figura 18) podemos resaltar una interfaz llamada Ut, definida por el 3GPP, que interconecta el UE directamente con el AS. Hay que aclarar que esta interfaz no se utiliza para invocar un servicio. Para esto ya existe la interfaz Gm, que está basada en SIP e interconecta directamente el UE con el P-CSCF del núcleo IMS.

La interfaz Ut proporciona al usuario un protocolo para configurar y gestionar aspectos relacionados directamente con el servicio del AS (por ejemplo, grupos o políticas). El protocolo propuesto por el 3GPP para esta interfaz es el XCAP (*XML Configuration Access Protocol*) en conjunción con el protocolo HTTP. Así pues, para el usuario, la interfaz Ut se puede traducir en una página web específicamente diseñada para la configuración del servicio del cual el usuario es suscriptor.

Protocolo XCAP

El protocolo XCAP, definido en el RFC 4825, es un protocolo que define cómo usar HTTP para crear, modificar y eliminar un documento XML incluyendo todos sus elementos, atributos y/o valores.

Figura 18. Interconexión lógica entre núcleo IMS y los servidores de aplicación (AS).



El caso expuesto en la Figura 18 en cuanto a la interconexión entre el S-CSCF y el AS vía la interfaz ISC, basada en SIP, es solo un caso genérico de interconexión. La realidad es que hay operadores que han apostado por una migración escalonada de su infraestructura a IMS para así amortizar los servidores de aplicaciones ya existentes y por lo tanto los servicios que ofrecen estos servidores no están basados en el protocolo SIP. Los protocolos usados en estos casos son por ejemplo el CSE de CAMEL (*Customized Applications for Mobile network Enhanced Logic service environment*) u OSA (*Open Service Architecture*).

Protocolo OSA

OSA responde a las siglas en inglés de *Open Service Access*. Es un marco que habilita las aplicaciones que implementan servicios a usar funcionalidades de red. Estas funcionalidades de red se traducen en las SCF o *Service Capabilities Features*, las cuales son accesibles a las aplicaciones a través de la API estandarizada de OSA para el desarrollo de servicios.

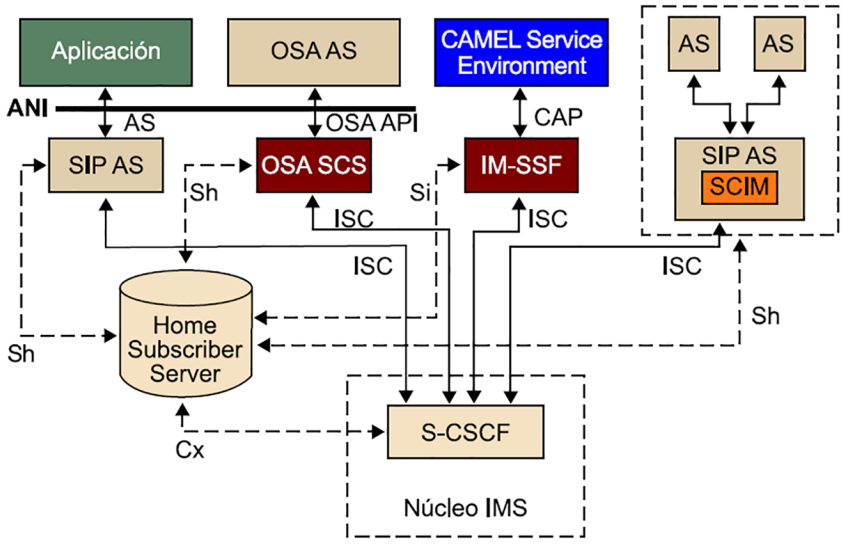
Ante este problema, el 3GPP ha aportado su particular visión a la capa de aplicación como se va a explicar a continuación.

Propuesta del 3GPP para la integración de AS en IMS

El 3GPP ha desarrollado conjuntamente una serie de especificaciones para la integración de los servicios en IMS.

En la Figura 19 se pueden observar los elementos que el 3GPP define para poder interconectar al núcleo IMS varios tipos de servidores de aplicación, los cuales vamos a describir brevemente a continuación.

Figura 19. Modelo de arquitectura de servicio NGN para 3GPP.



Para la provisión de estos servicios a los suscriptores de IMS, es necesaria una adaptación dentro del correspondiente servidor de aplicaciones. De esta forma, el término servidor de aplicaciones se emplea genéricamente para englobar tanto a los servidores nativos de SIP (SIP AS) como a los que proporcionan aplicaciones de CAMEL (*IP Multimedia Service Switching Function*, IM-SSF) para servicios de telefonía móvil (GSM o UMTS) u OSA (OSA *Service Capability Server*, SCS) para servicios de telefonía fija. Existen por tanto tres tipos de funciones de servidor de aplicaciones:

1) SIP AS: Los servidores de aplicaciones basados en SIP (SIP AS) son los servidores de aplicaciones nativos de IMS y, por lo tanto, no requieren de ningún tipo de adaptación en su interfaz con el S-CSCF del núcleo IMS (ver la Figura 19). Se puede afirmar que estas aplicaciones son las genuinamente creadas para interactuar con la capa de control de servicio de las redes NGN. Con lo cual todo nuevo servicio que se crease desde ahora se enmarcaría en este tipo de AS. Las atribuciones principales de un servidor de aplicaciones SIP son:

- Redirigir la sesión hacia redes o usuarios.
- Interactuar con las plataformas de servicios para el soporte de servicios avanzados.
- Comunicarse con el HSS para obtener información relativa a suscripciones o servicios.

Si el SIP AS se encuentra en la red local, la comunicación con el HSS se puede realizar mediante Diameter a través de la interfaz Sh, ya que se considera una interfaz intra-dominio.

Ejemplos de SIP AS son habilitadores como los servidores de presencia, de mensajería, de conferencia, de aplicaciones de llamada o también aplicaciones domésticas, de IPTV, de facturación, de descubrimiento de otros servicios, etc.

2) OSA AS - OSA SCS: El entorno OSA facilita diversas funcionalidades a los operadores, tales como control de llamadas, interacción del usuario, información de estado, información de la capacidad del terminal, control de sesiones de datos, gestión de cuentas o facturación. Otra ventaja del entorno OSA es que cuenta con funcionalidades de autenticación, autorización, registro y descubrimiento de servicio, por lo que es una forma eficaz de introducir en el sistema servidores de aplicaciones externos a la red IMS (el núcleo IMS no ofrece soluciones seguras para estos casos).

Dado que estos servidores de aplicaciones no soportan SIP, es necesaria la intermediación del OSA SCS (OSA *Service Capability Server*), con el objetivo de que maneje la señalización procedente del S-CSCF. De manera específica, el OSA SCS es la entidad que ejerce de interconexión entre:

- funciones de las redes NGN
- todos los servidores de aplicación externos con respecto al dominio local y
- los habilitadores de servicio.

La comunicación entre el OSA SCS y el OSA AS se lleva a cabo mediante una API específica.

3) CAMEL CSE (SCP) - IM SSF: Del mismo modo, a través de una red IMS también se puede acceder a servicios CAMEL de red inteligente (IN) y a sus funcionalidades, como la máquina de estados finitos para la conmutación de servicios (CAMEL *Service Switching Finite State Machine*), o los puntos de detección de activación de servicio (*trigger detection points*). El soporte de este tipo de aplicaciones implementadas en CSE (*CAMEL Service Environment*) en un entorno SIP se consigue gracias a la introducción de la IM-SSF (*IP Multimedia Service Switching Function*), una pasarela que permite a los SCP (*Service Control Points*) de CAMEL controlar una sesión IMS. En una red interna, la comunicación segura entre el AS y la HSS se realizaría a través de una interfaz llamada MAP (*Mobile Application Part*).

Interfaz MAP

MAP o *Mobile Application Part* es un protocolo SS7 que proporciona una capa de aplicación para los distintos nodos en las redes móviles troncales de GSM y UMTS para comunicarse mutuamente con el objetivo de proporcionar servicios a los usuarios de teléfonos móviles.

SCP

Un SCP, en inglés Service Control Point, es un componente de las llamadas Redes Inteligentes o IN (*Intelligent Networks*, en inglés) de los sistemas de telefonía tradicional (basados en SS7), el cual tiene como función el control de los servicios. Ejemplos de estos servicios son las llamadas prepago, cobro revertido, transferencia de llamada o portabilidad del número telefónico. La capa de aplicación de las redes inteligentes (IN) se hace llamar en inglés INAP o *Intelligent Network Application Part*.

4.4. Orquestación entre servicios y/o habilitadores

La orquestación entre los servicios es crucial, no solo en la creación de nuevos servicios de valor añadido, sino también para permitir una migración progresiva de los servicios ofrecidos hoy en día por los proveedores de servicios de comunicaciones (no basados en redes NGN) hacia servicios basados en IMS.

Este último factor es importantísimo, ya que las compañías que ya han invertido mucho dinero en la infraestructura de provisión de servicio actual (por ejemplo, en servicios basados en infraestructura heredada, como CAMEL o IN) necesitan amortizar su inversión. Así pues, se prevé una larga coexistencia entre los nuevos servicios generados (basados en IMS) y los que ya existen para, poco a poco, ir migrando la infraestructura.

De esta manera, dicha compañía podrá seguir dando servicio a los usuarios que aún siguen usando la infraestructura (telefonía móvil 2G/3G, RTC, RDSI) y servicios antiguos mientras va creando nuevos servicios amparados en el marco que ofrecen las redes NGN e IMS. Este es un factor clave que puede provocar que dichas compañías proveedoras se decidan a invertir en la migración progresiva hacia un sistema más eficiente, atractivo y con menores costes de mantenimiento y operación, como son las NGN.

Realizar la orquestación de varios servicios en uno solo no es tarea fácil. El elemento que se encargue de realizar dicha función recibirá una petición (por ejemplo, en forma de petición SIP desde el S-CSCF vía la interfaz ISC) y tendrá que desencadenar y/o coordinar la comunicación entre componentes de servicios según se requiera. Además, se le añade la dificultad de tener que realizar en ciertas ocasiones traducciones de protocolos, ya que los componentes o servicios que forman el servicio final son de carácter heterogéneo y pueden requerir la utilización de distintos protocolos en una misma sesión de servicio (a nivel de comunicación entre componentes).

Así pues, la orquestación de servicios se presenta como uno de los aspectos clave en el futuro de las redes NGN y todos estos requisitos se concretan en un elemento que será crucial en la integración de servicios: el *Service Broker*, que veremos en la sección 4.4.2.

El ***Service Broker (SB)*** es un elemento de red que gestiona eficientemente la interacción y la composición de los servicios. El SB reside entre la capa de servicio y la red convergente, y está tradicionalmente desvinculado de los elementos de encaminamiento de llamadas y de los entornos de creación y ejecución de servicio.

Antes de describir con más detalle el *Service Broker*, veamos una de las funciones que el 3GPP ha definido en relación con las funciones que éste desempeña: la funcionalidad SCIM (*Service Capability Interaction Manager*).

4.4.1. Funcionalidad SCIM (*Service Capability Interaction Manager*)

El SCIM (*Service Capability Interaction Manager*) gestiona la provisión de servicios entre distintas plataformas de servidores de aplicaciones dentro de la arquitectura IMS. El propósito del SCIM es pues la coordinación de las capacidades de estos servicios, a nivel de la capa de aplicación. Se trata de una entidad independiente que, en caso de estar presente en la arquitectura, se encuentra situada entre el S-CSCF del núcleo IMS y los servidores de aplicaciones (AS).

El SCIM está definido en el 3GPP TS 23.002. A lo largo del proceso de estandarización de IMS, se han identificado diferentes posibles implementaciones de SCIM, de las cuales describiremos sólo la más típica: SCIM como *broker* SIP.

En este modo de funcionamiento el SCIM gestiona la interacción entre distintos componentes de servicios basados esencialmente en SIP, y que implementan proxys o agentes de usuario (*user agents*). Para la gestión de esta interacción, el SCIM suele desempeñar funciones de B2BUA (agentes de usuarios interconectados entre sí en una misma entidad), y aplicar complejas secuencias de reglas y enrutamiento avanzado.

Estas secuencias de reglas son fijadas por los iFCs, que ya hemos explicado anteriormente.

4.4.2. El *Service Broker*

Al principio de este apartado ya hemos visto una pincelada del SB o *Service Broker* y ya podemos ver que no es un elemento que realice una tarea que se pueda considerar sencilla teniendo en cuenta los requerimientos que las compañías proveedoras de servicio necesitan. A modo de evolución del SCIM, el 3GPP también ha publicado un documento de especificación de definición del SB (TR 23.810), pero la última versión de dicha especificación (*Release 8*) deja en el aire numerosos aspectos como más tarde veremos. De todas formas, sí que podemos mencionar las dos funciones principales que un SB debe realizar:

1) Mediación entre servicios y la red: el SB proporciona toda la conectividad de red y la traducción de protocolos necesaria para soportar la interoperabilidad entre cualquier servicio de comunicación y cualquier red (incluyendo *Mobile Switch Center* o MSC de telefonía móvil, *switches* y *softswitches* de RTC, y S-CSCF del núcleo IMS). En este sentido, el SB va más allá que la funcionalidad SCIM explicada en el apartado anterior, la cual realiza esta misma función, pero solamente interconectando con el núcleo IMS en el lado de la red.

Como ejemplos, se puede mencionar el caso de mediación entre servicios de redes inteligentes (IN) pero de diferentes variantes de protocolos. También se puede dar el caso de la mediación entre servicios de IN y elementos de control de sesión IMS (el S-CSCF) o bien entre aplicaciones de NGN y elementos de control de llamada de redes tradicionales (el MSC de la red de telefonía móvil).

2) Orquestación de servicio en tiempo real: permite que múltiples servicios interactúen mutuamente dentro de una sola llamada o sesión, con el objetivo de poder crear nuevos servicios o agrupaciones de servicios combinando un número de servicios individuales (los cuales pueden estar asociados con redes heredadas o las redes NGN o una mezcla de ambas). Para ello usa las funcionalidades siguientes: SCIM, IM-SSF, gestión de *trigger* IN-IN, gestión de flujo de llamada/protocolo, facturación en tiempo real e interacción de datos de gestión de suscriptor (con HSS).

Para desempeñar estas funciones, el SB posee una arquitectura funcional interna que ayudará a entender cómo funciona este elemento. No obstante, como hemos comentado anteriormente, no hay una especificación clara de 3GPP sobre qué bloques funcionales conforman un SB. Ese hueco ha tenido que ser llenado por iniciativas de empresas privadas que ya han desarrollado sus propios SBs propietarios. Veamos entonces a continuación una propuesta genérica de dicha arquitectura, que puede dar una idea general de cómo podría estar implementado un SB.

Propuesta de arquitectura funcional

El SB estaría compuesto por los siguientes componentes, los cuales se pueden ver en la Figura 20:

1) Motor de orquestación: el MO reside en el corazón de la arquitectura del SB. El MO encamina las peticiones de servicios y tarificación desde la red a una o más plataformas de servicios. El MO además gestiona las interacciones entre plataformas de servicio y el encaminamiento de sesión a través de las aplicaciones.

2) Módulos de interacción (*Interworking Modules*): es un set de módulos configurables e intercambiables que habilitan al MO a comunicarse con plataformas de aplicaciones y entidades de control de sesiones en varias redes. Cada IM proporciona interacción con un elemento de red específico a través del protocolo nativo de dicho elemento. Existen tres tipos de IM:

IM-SSF

El IM-SSF, que interactúa con la aplicación, tiene su elemento espejo que interactúa con la red y que se llama IM-SSF inverso. El IM-SSF ya se ha descrito anteriormente. El IM-ASF inverso es el elemento espejo del IM-ASF (*Application Server Function*) que implementa la interfaz SIP para comunicarse con los SIP AS o habilitadores basados en este protocolo SIP de IMS.

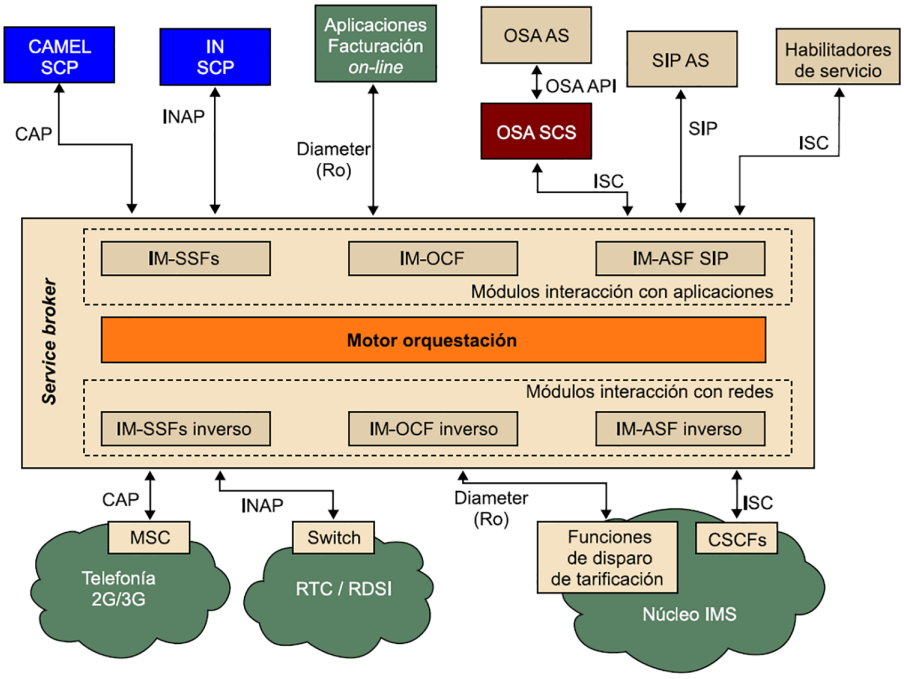
- **Módulos de interacción con las redes:** que habilitan conectividad entre el SB y las entidades de control de sesión, tales como MSC de telefonía móvil 2G/3G o el S-CSCF del núcleo IMS. Estos módulos proporcionan una interfaz inteligente a las entidades de control de sesión para que interactúen con el SB, de la misma manera en que interactúan con las plataformas de aplicación, sin necesidad de realizar cambios en configuración. Ejemplos de estos módulos son los IM-SSF inverso y los IM-ASF inverso (módulos de interacción con funciones de AS).

- **Módulos de interacción con las aplicaciones:** que habilitan la conectividad entre el SB y plataformas de aplicación, tales como los CAMEL IN, SIP AS y los servidores de tarificación *online*. Estos módulos proporcionan

una interfaz inteligente a las aplicaciones para que interactúen con el SB, de la misma manera que interactúan con la red, sin necesidad de realizar cambios en la configuración. Ejemplos de estos módulos son los IM-SSF, IM-OCF (módulo para la facturación *online*) y IM-ASF.

Módulos suplementarios: aunque no estén mostrados en la Figura 20, los módulos suplementarios son configurables e intercambiables facilitando y complementando las soluciones del SB en ciertos casos particulares. Estos módulos son proporcionados por el SB y pueden ser utilizados de manera opcional.

Figura 20. Arquitectura funcional de un *Service Broker.*



En el núcleo del SB, la interacción está normalizada a un modelo común de sesión y evento. Cada IM proporciona una conversión entre la representación de la sesión interna del SB y el protocolo externo aplicable. A través de un extenso abanico de IMS tanto de red como de aplicación, el MO extiende el servicio de orquestación más allá de IMS hacia servicios anteriores a IMS, como por ejemplo IN, redes SS7 y otros dominios no-IMS como IPTV o SOA. Todo esto posibilita la orquestación y la mediación entre varias plataformas de aplicación y tarificación.

Interacción del *Service Broker* con IMS

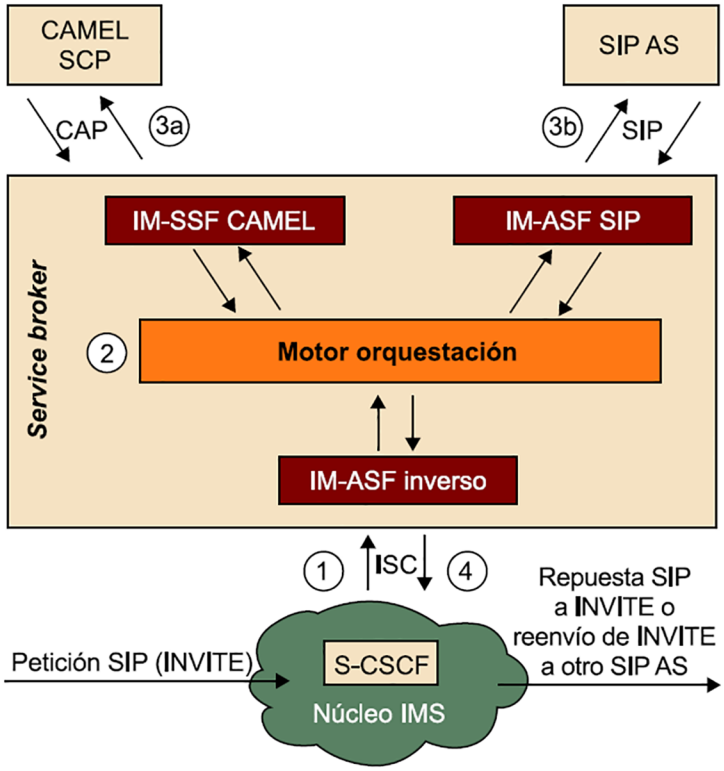
Como ya hemos visto en el anterior apartado, en el caso concreto de red IMS, el SB interactúa con el S-CSCF vía la interfaz ISC.

La orquestación de servicio dentro del dominio IMS está basada en un concepto de agregación de aplicaciones. Este concepto habilita la entrega de múltiples servicios en una sola sesión mediante el encaminamiento de la sesión a través de múltiples aplicaciones. La cadena de aplicaciones a través de la cual

pasa una sesión habilita a cada aplicación a cumplir su papel en el turno que le toque. El orden en que se recorren las aplicaciones depende de la lógica de la orquestación que más tarde veremos.

En la Figura 21 podemos ver un ejemplo de esta orquestación entre el núcleo IMS y el SB, la cual es disparada por una petición de SIP recibida desde el S-CSCF. Dentro del SB se produce la traducción de protocolos, accediendo primero al CAMEL SCP y luego al SIP AS antes de enviar la respuesta de vuelta al S-CSCF.

Figura 21. Ejemplo de orquestación mediante el *Service Broker*.



El MO gestiona la sesión como se indica a continuación:

1) El MO es activado a través del IM-ASF inverso por el S-CSCF al enviarle éste una petición SIP por la interfaz ISC (por ejemplo, un INVITE).

2) El MO encamina la sesión a múltiples aplicaciones a través de los módulos de interacción encarados a éstas. La ruta hacia múltiples aplicaciones no es estática, sino que es determinada en tiempo real por lógica de orquestación, la cual es seleccionada por el MO y descargada dinámicamente (por ejemplo, desde la base de datos de suscripciones o HSS vía la interfaz Sh, el MO se descarga los iFC del perfil de usuario para aplicar la lógica de orquestación).

3) El MO reenvía la sesión a la aplicación correspondiente según estas rutas dinámicamente configuradas.

4) Una vez la sesión ha pasado por la última aplicación en la cadena, el MO retorna la sesión al S-CSCF.

En este ejemplo (Figura 21), hemos propuesto como petición SIP un INVITE, pero no tiene por qué ser necesariamente este mensaje, ya que existen otras peticiones SIP como REGISTER, MESSAGE, SUBSCRIBE o NOTIFY.

Proceso de orquestación en el motor de orquestación

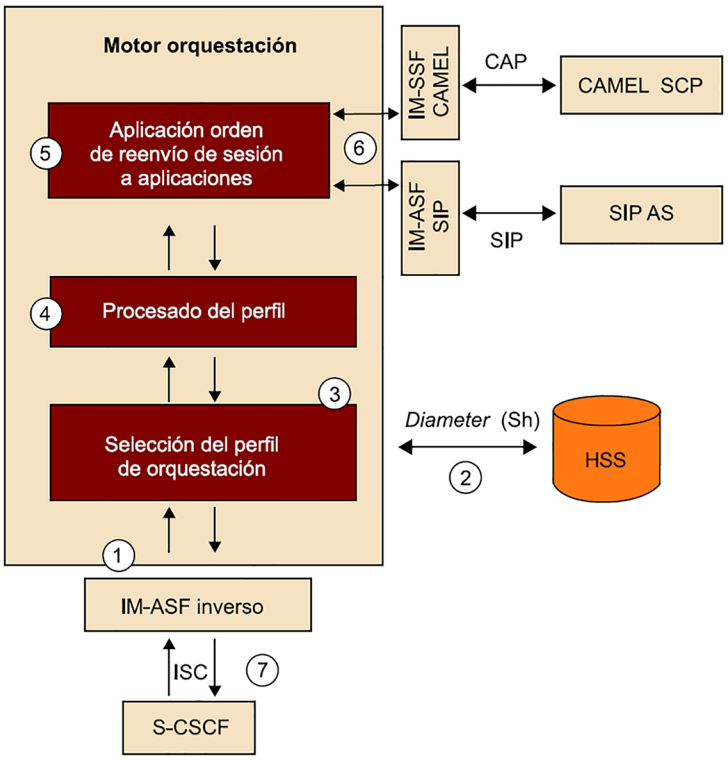
En la Figura 20 hemos visto que el MO es el corazón del SB. Pero veamos cómo funciona exactamente por dentro y qué procesos alberga para poder tomar las decisiones de orquestación cuando llega una petición de sesión.

Para realizar el servicio de orquestación, el MO requiere de una lógica de orquestación. Una lógica de orquestación define las aplicaciones a través de las cuales el MO debería pasar una sesión y el orden en que estas aplicaciones deben ser invocadas.

Queremos reiterar que no hay una especificación estandarizada sobre el diagrama de flujo en cuanto a funciones a desempeñar por el SB a la hora de realizar el proceso de orquestación. Son las empresas privadas las que han rellenado este hueco con propuestas propietarias. Con lo cual, lo que vamos a mostrar a continuación es una descripción genérica de las fases por las que pasaría el MO a la hora de aplicar la lógica de la orquestación.

El servicio de orquestación necesita realizar principalmente tres tareas las cuales se pueden ver dentro de la caja del MO en la Figura 22. En esta figura también se puede ver paso a paso cómo se aplican los perfiles orquestación desde que una petición de sesión llega desde el S-CSCF:

Figura 22. Aplicación en el MO de la lógica de orquestación.



HSS

El HSS contiene información de suscripción de los usuarios incluyendo las aplicaciones a usar, así como los perfiles de orquestación de estos (iFC almacenados en el perfil de suscripción).

(5)Opcionalmente, dichos perfiles pueden estar almacenados localmente en una base de datos en el mismo *Service Broker* en lugar de estar en el HSS (*Home Subscriber Server*).

1) El servicio de orquestación recibe una petición de sesión desde el elemento de control de sesión correspondiente (en este caso, del S-CSCF), que a su vez es reenviado al MO por el módulo de interacción.

2) El MO delega al módulo de obtención del perfil de orquestación (iFC) la función de selección del perfil. Para ello, éste se conecta vía la interfaz Sh con el HSS[5].

3) Basándose en la información contenida en el propio mensaje de petición de sesión recibido, el módulo de obtención del perfil selecciona el perfil de orquestación a utilizar para tal sesión y se lo transfiere al MO para su uso.

4) Dentro del MO, el módulo de procesamiento elabora el plan de reenvío de la sesión a las aplicaciones que sean necesarias y en el orden que sea necesario.

5) El MO ejecuta la lógica de orquestación invocando a la primera aplicación.

6) Cuando la primera aplicación devuelve el mensaje de sesión el MO invoca a la siguiente aplicación y así hasta que se cumpla toda la lista.

7) Cuando este proceso ha acabado se devuelve el mensaje de sesión al S-CSCF.

Ejemplo detallado de aplicación de los iFCs como lógica de orquestación en el caso particular de la funcionalidad SCIM (donde solo se realiza la orquestación con SIP AS)

Cuando entra en el SB (que tiene solo funcionalidad SCIM) una petición inicial de SIP reenviado desde el S-CSCF (por ejemplo, REGISTER, INVITE, SUBSCRIBE, MESSAGE, etc.) se realizan los siguientes pasos:

SCIM en el S-CSCF

La funcionalidad SCIM es relativamente común encontrarla integrada en la misma plataforma donde el S-CSCF se implementa.

Devolución de mensaje

Si el *Service Broker* (SCIM) no encuentra un *Service Profile* para un IMPU en concreto, devuelve el mensaje SIP de vuelta al S-CSCF sin modificar.

1) El SB selecciona el *Service Profile* (lista de IFCs a aplicar) según el IMPU asociado al suscriptor y si la llamada es entrante o saliente (*originating* o *terminating*). Es decir, si la llamada es sentido *originating*, el IMPU asociado al suscriptor se coge de la cabecera SIP *From:* y si es sentido *terminating* se coge de la cabecera SIP *To:*

2) Se comprueba empezando por el iFC de más alta prioridad (mirando el *priority level* del iFC) si el mensaje SIP reenviado desde el S-CSCF cumple con todos los *trigger points* que conforman dicho iFC.

3) Si no cumple, el SB consulta el siguiente iFC por orden de prioridad y así hasta que ya no queden iFCs por aplicar.

4) Si el mensaje SIP cumple con alguno de los iFC se reenvía al SIP AS asociado (SIP URI). Si el SIP AS devuelve el mensaje SIP (puede incluso que modificado) el SB sigue aplicando el resto de iFC de la lista desde el punto en que se había quedado y por orden de prioridad hasta que ya no queden iFCs por aplicar.

Cuando no quedan iFCs por aplicar, finalmente reenvía la petición SIP de vuelta al S-CSCF para que lo encamine al destinatario final.

4.5. Service Enablers o habilitadores de servicio de VoLTE

MMTel y los servicios suplementarios

El GSMA ha definido la especificación IR.92 y IR.94 para definir las características del servicio de telefonía en IMS para llamadas de voz y de video respectivamente tanto del lado del UE como del lado del *Application Server*. También ha definido el IR.51 para especificar las características del servicio de VoWi-Fi. Estas especificaciones buscan maximizar la interoperabilidad entre distintos fabricantes.

A continuación, describiremos los *service enablers* más comunes que podemos encontrar para proveer el servicio de VoLTE (al menos los ofrecidos por las empresas especializadas en provisión de *software* para este tipo de servicios IMS).

MMTel – *Multimedia Telephony*

TAS virtualizado

Muchos fabricantes de SIP AS están ofertando proporcionar su servidor de aplicaciones en formato VNF (*Virtualized Network Function*) de modo que puede ser utilizado en un entorno virtualizado que cumpla la especificación de la ETSI de NFV-MANO, que veremos en el siguiente módulo.

El servicio de telefonía multimedia de 3GPP/TISPAN (en inglés *Multimedia Telephony*) es un estándar basado en IMS (utiliza el protocolo IP para transporte y SIP para señalización de servicios), que permite a los usuarios establecer comunicaciones multimedia. Provee los siguientes servicios estandarizados:

- Conversación de voz bidireccional.
- Transmisión de video uni o bidireccional.
- Mensajería en texto
- Transferencia de ficheros
- Compartición de ficheros de audio, video y fotos.
- Capacidad de añadir o eliminar componentes multimedia (audio/video) según se necesite durante una sesión

Este habilitador de servicio es usado típicamente para implementar servidores de telefonía (TAS o *Telephony Application Server*) en los que se ofrecen los servicios de emulación de red GSM (es decir, implementación de todos los servicios telefónicos que ya venían) y servicios suplementarios para llamadas VoLTE y VoWi-Fi (especificados en los perfiles del GSMA IR.92, IR.94 y IR.51). Como servicios suplementarios podemos encontrar entre otros: transferencia de llamada automática, bloqueo de llamada, identificación del llamante, llamada en espera, etc.

SCC – *Service Centralization & Continuity*

SCC

El GSMA publicó la especificación IR.64 donde describe cómo debe ser el servicio SCC.

El servicio de centralización y continuidad utiliza métodos definidos por 3GPP como parte de *IMS Centralized Services* (ICS) para anclar las llamadas en este servidor asegurando coherencia en la sesión tanto si acceden desde el dominio de conmutación de circuitos (CS) o desde conmutación de paquetes (PS). Para todas las llamadas que están ancladas, el SCC-AS actúa como un B2BUA estableciendo las vertientes de las llamadas a todos los puntos finales desde el SIP INVITE hasta el SIP BYE.

SRVCC y eSRVCC

La diferencia entre uno y otro es que el primero solo ancla la llamada a nivel de señalización (solo mensajes SIP) mientras que el segundo implementa también un anclaje a nivel de flujos multimedia (flujos de voz y/o video).

Este habilitador se encuentra en la implementación de servidores de aplicaciones de continuidad de llamada de voz (VCC o *Voice Call Continuity*). El VCC permite la continuidad de una sesión de voz cuando el usuario se mueve con su teléfono entre LTE y redes no-LTE de tipo *Circuit Switched* (CS) en los que se utilizan tecnologías como GSM (*Global System for Mobile Communications*) y UMTS (*Universal Mobile Telecommunication System*). A este servicio también se le llama comercialmente SRVCC (*Single Radio Voice Call Continuity*) aunque han aparecido nuevas versiones mejoradas como el eSRVCC (*enhanced Single Radio Voice Call Continuity*).

CONF – *Multiparty Conference Call*

Este habilitador ofrece la capacidad de establecer y enlazar múltiples sesiones multimedia. Normalmente existe la parte que gestiona exclusivamente la señalización de las sesiones que es implementada en un SIP AS mientras que para el procesado de los flujos multimedia se utiliza el elemento específico que da esta función en el núcleo IMS, el MRF. El servicio de multiconferencia para VoLTE está especificado en el IR.92 del GSMA.

Normalmente este servicio está incluido en el TAS aunque se puede implementar como un servidor por separado.

Group messaging

Este habilitador proporciona mensajería instantánea ya sea 1-a-1 o en grupo y ha sido estandarizado por varias entidades y cada una le asigna un nombre distinto: el IETF lo llama *Instant Messaging*, el 3GPP IMS *Messaging* y el OMA SIMPLE *Instant Messaging*. No obstante, el más usado es el que le ha otorgado el GSMA; RCS o *Rich Communication Service*.

Curiosidad sobre RCS

El GSMA bautizó la primera versión de RCS (en el año 2012) con el nombre de *joyn.*

El RCS incluye además otros servicios como agenda de contactos, llamadas de voz y video *best effort*, compartición de contenidos y ficheros, etc.

El RCS viene a ser el equivalente a *Whatsapp*, pero implementado para IMS.

Resumen

Las redes NGN nos muestran un nuevo paradigma de convergencia de redes de transporte y de independencia de los servicios con respecto a estas redes, todo ello con el protocolo IP como piedra angular. Ofrecen un marco en el que los proveedores de servicio pueden desarrollar nuevas aplicaciones y servicios sin preocuparse de la tecnología subyacente en el equipo de usuario (UE). Además, las redes NGN garantizan la calidad de servicio (QoS) extremo a extremo, ofreciendo interoperabilidad con redes y servicios existentes hoy en día (RTC / RDSI o telefonía móvil).

Hoy en día ya existen operadores que han invertido e implementado redes y servicios que cumplen con NGN como por ejemplo la red de *LTE Advanced* y el servicio de VoLTE. Es precisamente el mercado de la telefonía móvil la que está impulsando, de la mano del 3GPP, nuevas especificaciones y modelos de referencia que abstraen cada vez más los servicios de la tecnología de red, como ya está sucediendo con la especificación de 5G.

En cuanto a la **capa de transporte**, LTE es una red de acceso especificada por el 3GPP que ofrece las características de las NGN. La interacción de esta capa con el núcleo IMS (capa de servicio) es gracias a la subcapa de procesado de transporte protagonizado por el PCRF que controla la definición de las reglas PCC. Estas reglas marcan el comportamiento del tráfico IP a nivel de QoS cuando atraviesan el EPC (*Evolved Packet Core*).

Otras tecnologías inalámbricas como Wi-Fi han sido incorporadas para que puedan integrarse con el EPC y ofrecer a los operadores de telefonía móvil una manera natural de extender su cobertura más allá de sus dominios administrativos. 3GPP ha incluido dicha integración en sus modelos de referencia para dar forma al servicio VoWi-Fi.

También cada vez más aparecen tecnologías que integran servicios web y comunicaciones multimedia, especialmente webRTC. En este caso, 3GPP también ha hecho un esfuerzo en integrarlo.

Respecto a la **capa de servicio**, el 3GPP ha definido el núcleo IMS, el cual se basa en la definición por una parte de unas entidades funcionales (CSCF) que procesan y encaminan los mensajes de establecimiento de sesión de servicios, y en una segunda parte de elementos de almacenaje de información de suscripción de usuario a nivel de servicio (HSS). Estos mensajes están basados en el protocolo SIP (definido por el IETF) pero con unas extensiones en su definición para adaptarse a IMS. Con el protocolo SIP un usuario puede invocar una sesión de cualquier servicio multimedia (voz o videoconferencia) sirvién-

dose de otros protocolos encapsulados en la propia señalización SIP, como por ejemplo SDP, que se usa para negociar parámetros de QoS extremo a extremo con el otro usuario o servidor de aplicación o AS.

A nivel de **capa de aplicación**, la entidad que mejor representa un servicio NGN/IMS es el servidor de aplicaciones (AS), el cual se interconecta al elemento de control de sesión del núcleo IMS (S-CSCF) con una interfaz basada en el protocolo SIP llamada ISC (*IMS Service Control*). Desde el punto de vista del núcleo IMS, la manera de saber hacia qué servidor de aplicaciones (AS) redirigir una petición SIP es acceder a la base de datos de suscripciones (HSS) y obtener las iFC o initial Filter Criteria asociadas al perfil de servicio del usuario. Los iFC contienen información que le dice al S-CSCF hacia qué AS hay que enviar una petición SIP en función de los valores de ciertos campos de la cabecera del propio mensaje.

Los servicios NGN se adaptan al paradigma SOA, el cual se basa en la integración de componentes de servicios más sencillos, reutilizables, independientes entre sí y autocontenidos para poder crear fácilmente nuevos servicios de valor añadido. A estos componentes se les llama habilitadores de servicios o *service enablers*. Varios ejemplos de estos habilitadores reutilizables son los servicios de presencia o gestión de lista de grupos.

Cuando hablamos de integración de servicio, obligatoriamente tenemos que hablar de la coordinación y orquestación de componentes de servicio, y es aquí donde surge un elemento clave en la provisión de servicios NGN: el *Service Broker o SB*.

El SB es un elemento de red que gestiona eficientemente la interacción y la composición de los servicios. El SB reside entre la capa de servicio (servidores de aplicaciones y habilitadores de servicio) y la red convergente (representado por el núcleo IMS), y está tradicionalmente desvinculado de los elementos de encaminamiento de llamadas y de los entornos de creación y ejecución de servicio. La lógica de orquestación es algo que el SB puede obtener de la HSS o de políticas propias.

Ejercicios de autoevaluación

1. A continuación, mostramos una lista de definiciones de bloques funcionales que están incluidos en el núcleo IMS definido por el 3GPP.

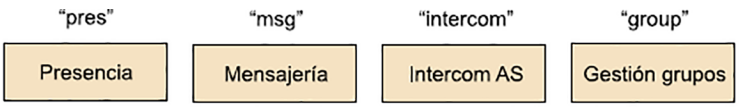
a) Es el elemento frontera del núcleo IMS que se conecta directamente con el usuario (cliente IMS) y por lo tanto el primer SIP proxy que recibe y procesa las peticiones SIP.
b) Es el elemento que hace frontera con otros núcleos IMS de otros operadores. Cuando un mensaje SIP debe encaminarse hacia otro dominio, pasa por este elemento justo antes de salir hacia el elemento homólogo del otro dominio administrativo.
c) Es el elemento central del núcleo IMS donde los clientes se registran. Además, es donde se mira por primera vez el Request-URI (destino final del mensaje SIP) para tomar la decisión de encaminamiento hacia otro dominio IMS, hacia un Servidor de Aplicaciones (AS) o hacia otra red heredada (RTC, por ejemplo).
d) Es un SIP proxy que se encarga de encontrar el S-CSCF correcto de un usuario en concreto (consultando el HSS) y encaminar el mensaje SIP hacia éste. Uno de los elementos que más lo consulta es el P-CSCF.
e) Es el elemento que hace de frontera con redes RDSI o RTC. Por un lado, recibe y procesa las peticiones de sesiones SIP que recibe desde el BGCF para convertirlas en peticiones equivalentes en las redes heredadas. Viene a ser como una VoIP a nivel de señalización.

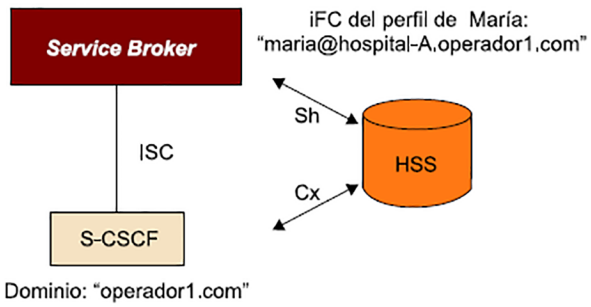
La lista de elementos es la siguiente:

1. I-CSCF
2. IBCF
3. P-CSCF
4. MGCF
5. S-CSCF
6. BGCF

Relaciona cada una de las definiciones con uno de los elementos. (NOTA: hay un elemento extra en la segunda lista que no se debe utilizar).

2. Tenemos el hospital A que quiere dar un servicio de atención remota a personas de la tercera edad que están en su casa. Cada paciente dispone de un dispositivo colgado del cuello que tiene dos botones: un botón rojo para que al pulsarlo el hospital se dé cuenta de que su estado ha cambiado a "no me encuentro bien", y un botón azul para poder hablar directamente con una enfermera (que permanentemente está escuchando) sin necesidad de llamar por teléfono. El hospital ha contratado al operador1.com para disponer en su dominio a todos los pacientes registrados, así como tener asociado su servicio de atención remota. En la siguiente figura se muestran los componentes que están a disposición del hospital para poder proporcionar cualquier servicio:





Contestad a las siguientes preguntas:

a) ¿Qué papel tiene el *Service Broker*?
b) Mirando la figura anterior, ¿qué componentes creéis que se usarían en este servicio de atención a gente de la tercera edad?
c) ¿Qué mensajes SIP creéis que el aparato de aviso utilizará según el botón pulsado?

d) Viendo la figura, ¿qué componentes creéis que debería integrar el *Service Broker* para este caso?

e) Para una paciente llamada María que tiene su perfil almacenado en el HSS, proponed los iFC almacenados para ser consultados por el S-CSCF de núcleo IMS.

f) Haced lo mismo para el caso del *Service Broker* para la orquestación del servicio.

Solucionario

1.

a) P-CSCF
b) IBCF
c) S-CSCF
d) I-CSCF
e) MGCF

2.

a) El Service Broker integra y coordina varios servicios elementales en uno solo de mayor valor añadido. Para el usuario la complejidad del servicio queda enmascarada, ya que solo existe un servidor de aplicación con el que interactuar, el representado por el *Service Broker*: PSI URI: servicio-atención-remota@hospital-A.operador1.com

b) Se detectan dos servicios que conjuntamente pueden formar este nuevo servicio: primero el servicio de presencia, que al apretar el botón rojo su estado en dichos componentes cambie a "no me encuentro bien" para que el personal dedicado del hospital pueda verlo (un enfermero o una enfermera). El segundo servicio es el de Intercom (llamada que va siempre al mismo destino), que se activaría con el botón azul. Este servicio, establece directamente una conexión de voz con un enfermero o una enfermera sin necesidad de marcar ningún número.

c) Para el servicio de cambio de estado sería un mensaje NOTIFY con el nuevo estado lo que enviaría al servidor de aplicación (representado por el *Service Broker*). Para el servicio de llamada estática sería un mensaje INVITE.

d) Solo se necesitaría dos componentes: el de presencia, donde se enviarían los NOTIFY y el servidor de aplicación llamado Intercom que recibiría el INVITE de inicio de llamada.

e) El iFC del perfil de María que necesita el S-CSCF para enviar los NOTIFY a *Service Broker* sería:

Método SIP	NOTIFY
OR	
Método SIP	INVITE
AND	
Cabecera SIP **Valor cabecera SIP**	To: .*hospital-A.operador1.com.*

f) Habrá dos iFC, uno de cada tipo de método:

iFC de presencia asociado al AS pres@hospital-A.operador1.com

Método SIP	NOTIFY
AND	
Cabecera SIP **Valor cabecera SIP**	To: pres@hospital-A.operador1.com

iFC de presencia asociado al AS intercom@hospital-A.operador1.com

Método SIP	INVITE
AND	
Cabecera SIP **Valor cabecera SIP**	To: intercom@hospital-A.operador1.com

Glosario

3GPP *Third Generation Partnership Project*. Entidad estandarizadora de tecnología móvil. Entre otras, UMTS y LTE así como IMS.

AF *Application Function*. Desde el punto de vista de la red de transporte el AF simboliza el elemento de la capa de servicio que tiene contacto directo con los elementos de la subcapa de control de transporte.

ARP *Allocation and Retention Priority*. Parámetro que indica la importancia o nivel de prioridad de un IP-CAN bearer.

AS *Application Server*. Elemento que provee un servicio en las redes NGN.

AVP *Attribute Value Pair*. En el protocolo Diameter y en un contexto de redes NGN, representan a parámetros que contienen información sobre una sesión de reserva de recursos.

B2BUA *Back-to-Back User Agent*. Son dos agentes de usuario SIP en la misma máquina, pero interconectados entre sí por algún tipo de lógica o funcionalidad

BBERF *Bearer Binding and Event Reporting Function*. Función de asociación de bearers y reporte de eventos en el modelo de referencia PCC del 3GPP.

BGCF *Breakout Gateway Control Function*. Elemento definido en el núcleo IMS el 3GPP que se encarga de seleccionar el siguiente salto de una petición SIP cuando la dirección de destino de la llamada no es un identificador típico SIP URI.

CAMEL *Customized Applications for Mobile networks Enhanced Logic*. Es un set de estándares definidos por la ETSI y 3GPP diseñados para permitir al operador definir servicios sobre el estándar de servicios GSM y de servicios UMTS

CSE CAMEL *Service Environment*. Describe el entorno CAMEL para el entorno de creación de servicios y para los nodos dentro de la red que interactúan para entregar servicios al suscriptor.

DIAMETER Evolución del protocolo RADIUS para el desarrollo de aplicaciones de AAA.

DNS *Domain Name Server*. Servidor de resolución de nombres de host a dirección IP.

E-CSCF *Emergency Call Session Control Function*. Componente del núcleo IMS que ejerce de elemento que procesa una llamada IMS de emergencia. Es un elemento definido por el 3GPP.

EPC *Evolved Packet Core*. Red troncal de la red LTE según el 3GPP.

EPS *Evolved Packet System*. Modelo de referencia de la 3GPP para la capa de transporte tanto en la parte de red troncal (EPC) como de red radio (E-UTRAN).

EPS *bearer* *Evolved Packet System Bearer*. Canal virtual con unas características de QoS y ancho de banda particulares desde la PDN-GW hasta el terminal de usuario (modelo de referencia del PCC del 3GPP).

ETSI La *European Telecommunications Standards Institute* es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial. http://www.etsi.org

E-UTRAN *Evolved UMTS Terrestrial Radio Access*. Definición de la red radio de LTE según el 3GPP.

GBR *Guaranteed Bit Rate*. Tasa garantizada de bit (usado como parámetro de caracterización de los IP-CAN bearer).

GERAN *GSM Edge Radio Access*. Definición de la red radio de GPRS según el 3GPP.

GPRS *General Packet Radio Service*. Es una extensión del GSM para la transmisión por paquetes que permite velocidades de transferencia de 56 a 144 kb/s.

GSM *Global System for Mobile communications*. Estándar de telefonía móvil de segunda generación.

GTP *GPRS Tunneling Protocol*. Protocolo de entunelado IP usado en GPRS para el transporte de paquetes IP.

HLR *Home Location Register*. En el mundo de la telefonía móvil, es una base de datos que almacena información de suscripción y de localización de usuarios.

HSS *Home Subscriber Server*. Base de datos que almacena la información de suscripción de un usuario junto con información de autenticación y autorización a nivel de servicio (modelo de referencia del 3GPP).

HTTP *HyperText Transfer Protocol*. Es el protocolo usado en cada transacción de la WWW.

HTTP *Digest* Mecanismo de autenticación que utiliza MD5 como hash y que es usado en autenticación en servicios web.

IBCF *Interconnection Border Control Function*. Función de control de pasarela fronteriza con otra red de troncal, dentro del modelo de referencia del 3GPP y de la ETSI-TISPAN en el núcleo IMS.

I-CSCF *Interrogating Call Session Control Function*. Componente del núcleo IMS que ejerce de elemento de encaminador de la señalización SIP hacia el S-CSCF correcto dentro de su mismo dominio. Es un elemento definido por el 3GPP.

IETF *Internet Engineering Task Force* es una entidad de estandarización abierta responsable de la mejora de los protocolos y los estándares que definen la tecnología de Internet.

IMPI *IP Multimedia Private Identity*. Representa la identidad privada de un usuario.

IMPU *IP Multimedia Public Identity*. Representa la identidad pública de un usuario.

IMS El *IP Multimedia Subsystem* es el estándar definido por el 3GPP para proveer servicios multimedia en telefonía móvil basados en protocolos definidos por IETF (SIP, RTP o Diameter).

IMS AKA *IMS Authentication and Key Agreement*. Se basa en una clave secreta de larga duración compartida entre el ISIM y el centro de autenticación de la red de acceso.

IN *Intelligent Networks*. Plataforma basada en la interconexión de nodos de redes de conmutación de circuitos en donde residen aplicaciones informáticas, centrales de conmutación y sistemas de bases de datos en tiempo real, enlazados mediante avanzados sistemas de señalización, para proveer la nueva generación de servicios.

IP *Internet Protocol*.

IP-CAN *Internet Protocol Connectivity Access Network*. Red de acceso que proporciona conectividad IP.

IP-CAN *bearer* Canal virtual de un IP-CAN.

IPTV *IP Television*. Servicio de televisión basado en el protocolo IP. Puede estar basado en IMS o definir su propia plataforma de gestión y control del servicio.

ISIM Significa *IMS Subscriber Identity Module*, una tarjeta *smart card* con información sobre la identidad de un usuario IMS.

ITU-T *International Telecommunications Union-Telecommunication*. Sector de normalización de las telecomunicaciones de la ITU en que se establecen normas que comprenden desde la funcionalidad básica de la red y la banda ancha hasta los servicios de las redes de próxima generación.

LTE *Long Term Evolution*. Definida por el 3GPP para la evolución de la telefonía móvil..

MBR *Maximum Bit Rate*. Tasa de bit máxima (usado como parámetro de caracterización de los IP-CAN bearer).

MGCF *Media Gateway Control Function*. Función de control de pasarela de medios en el modelo de referencia de la 3GPP en el núcleo IMS.

MME *Mobility Management Entity*. Entidad que gestiona la movilidad de los terminales de usuario en la red radio del modelo EPS (modelo de referencia del 3GPP).

MO Motor de Orquestación en el *Service Broker*.

MRB *Multimedia Resource Broker*. Función de gestión de recursos de medios en el modelo del 3GPP en el núcleo IMS.

MRFC *Media Resource Function Control*. Función de control de recursos de medios en el modelo de referencia del 3GPP y ETSI-TIPAN en el núcleo IMS.

MRFP *Media Resource Function Processor*. Función de procesado de recursos de medios en el modelo de referencia de la ETSI-TISPAN y del 3GPP en el procesado de transporte.

NAPT *Network Address and Port Translation*. Traducción de puertos y direccionamiento IP.

NAT *Network Address Translation*. Traducción de direccionamiento IP entre un direccionamiento privado y otro público.

NGN Responde a las siglas de *Next Generation Networks* y es como se denominan las redes de próxima generación.

NNI *Network-Network Interface*. Define la frontera entre dos redes distintas (dos redes troncales o una red troncal y una red de acceso).

NSWO *Non-Seamless WLAN Offload*. Es una prestación definida por el 3GPP la cual indica al terminal móvil que para llamadas IMS use la interfaz SWu (túnel IPSec) pero para tráfico no-IMS use directamente la Wi-Fi de manera transparente.

OCS *Online Charging System*. Sistema de control de facturación en línea, para controlar en tiempo real el gasto en un servicio. Elemento dentro del modelo de referencia PCC del 3GPP.

OFCS *Offline Charging System*. Sistema de control de facturación diferido, para la posterior generación de las facturas de uso de un servicio. Elemento dentro del modelo de referencia PCC del 3GPP.

OFDMA *Orthogonal Frequency-Division Multiple Access*. Versión multiusuario de la Multiplexación por División de Frecuencias Ortogonales o OFDM.

OMA Responde a las siglas de *Open Mobile Alliance* y desarrolla estándares abiertos para la industria de telefonía móvil. http://www.openmobilealliance.org

OSA/Parlay *Open Service Access* / Parlay. Es una API (*Application Programming Interface*) para el acceso de aplicaciones a los recursos de las redes de telecomunicaciones.

PCC *Policy Control and Charging*. Control de las políticas de QoS y de facturación, definidas en el modelo de referencia del 3GPP para el control de la red de transporte.

PCEF *Policy and Charging Enforcement Function*. Función de aplicación de políticas y facturación en el modelo de referencia PCC del 3GPP.

PCRF *Policy Charging and Rules Function*. Grupos de funciones que conforman el control de admisión y recursos del modelo de referencia PCC del 3GPP.

P-CSCF *Proxy Call Session Control Function*. Componente del núcleo IMS que ejerce de elemento fronterizo con el equipo de usuario a nivel de señalización SIP, definido por el 3GPP.

PDN GW *Packet Data Network Gateway.* Elemento del EPC frontera que interconecta con la red troncal de otro operador.

PSI *Public Service Identifier*. Es un identificador de servicio público que identifica a cualquier elemento de destino de una llamada SIP y que no es un usuario.

QCI *QoS Class Identifier*. Parámetros que define el comportamiento de QoS del tráfico asociado a un *bearer* de EPS.

QoS Término que califica la calidad de servicio o *Quality of Service*.

RADIUS *Remote Authentication Dial-In User Server*. Es un protocolo definido por el IETF de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

RDSI Red Digital de Servicios Integrados.

REST *Representational State Transfer*. Conjunto de principios de arquitectura para describir cualquier interfaz entre sistemas que utilice directamente HTTP para obtener datos o indicar

la ejecución de operaciones sobre los datos, en cualquier formato (XML, JSON, etc.) sin las abstracciones adicionales de los protocolos basados en patrones de intercambio de mensajes.

RFC *Request For Comment*. Donde se plasman por escrito los estándares que define la IETF.

RTC Red Telefónica Conmutada.

RTP *Real Time Protocol*. Protocolo basado en UDP para la transmisión de flujos multimedia (audio, vídeo) en tiempo real.

SAE *System Architecture Evolution*. Forma equivalente de llamar al EPS.

SBC *Session Border Controller*. Elemento colocado en las fronteras administrativas de una red gestionada o dominio (ejemplos de SBC: P-CSCF o IBCF).

SCIM *Service Capability Interaction Manager*. Funcionalidad propuesta por el 3GPP para la orquestación de servicios y habilitadores cuando el servicio se invoca desde el núcleo IMS (en concreto desde el S-CSCF).

S-CSCF *Serving Call Session Control Function*. Componente del núcleo IMS que ejerce de registrador del usuario a nivel de capa de control de servicio y de encaminador de la señalización hacia otros elementos que finalicen la llamada dentro del mismo dominio o de otro distinto. Es un elemento definido por el 3GPP.

SDP *Session Description Protocol*. Protocolo adherido a la señalización SIP para negociar parámetros multimedia de establecimiento de sesión (códecs o puertos UDP donde enviar los flujos RTP).

SGSN/GGSN *Serving GPRS Support Node/Gateway GPRS Support Node*. En una red troncal GPRS el SGSN se encarga de la parte de movilidad del celular además de dar acceso a estos a la red de datos móviles, de autentificar y asignar la calidad del servicio a utilizar por cada terminal. El GGSN es la puerta de enlace o punto central de conexión hacia el exterior o la PDN (Packet Data Network) de una red celular (red móvil), estas redes externas pueden ser Internet o una red corporativa.

SGW *Serving Gateway*. Componente del EPC del 3GPP que hace de anclaje de las conexiones IP para garantizar el servicio de movilidad en terminales móviles.

SIP El *Session Initiation Protocol* es un protocolo definidos por el IETF para el establecimiento y negociación de sesiones de servicios multimedia.

SLA *Service Level Agreement*. Define las características del servicio para un suscriptor.

SLF *Subscriber Location Function*. Elemento del modelo de referencia de IMS del 3GPP que se encarga de encontrar la HSS correcta donde se ubica un perfil de usuario buscado.

SOA *Service Object Architecture*. Estilo arquitectural cuyo objetivo es conseguir el desacoplo entre los componentes de *software* que interactúan entre sí.

SOAP *Simple Object Access Protocol*. Es un protocolo simple basado en XML para el intercambio de información en un entorno distribuido y descentralizado.

SPR *Subscription Profile Repository*. Función de almacenamiento de perfiles de usuario a nivel de capa de transporte en el modelo PCC del 3GPP.

SS7 *Signalling System number 7*. Sistema de señalización nº 7 usado en los enlaces troncales de telefonía.

TCP *Transport Control Protocol*. Protocolo de capa 4 para enviar paquetes con confirmación.

THIG *Topology Hiding Inter-network Gateway*. Funcionalidad de enmascaramiento de topología de red que elimina de las cabeceras SIP cualquier información que pueda revelar la topología de la red.

UA *User Agent*. En el protocolo SIP, representa el punto inicial o de terminación de un mensaje SIP. Normalmente, es implementado por un cliente o un servidor de aplicaciones SIP (SIP AS).

UDDI *Universal Description Discovery and Integration*. Elemento de la arquitectura SOA que se usa para que proveedores de servicio puedan registrar información sobre los servicios que ofrecen y hacerlos públicos.

UDP *User Datagram Protocol*. Protocolo de capa 4 para enviar paquetes sin confirmación.

UE Equipo de usuario. Puede contener uno o más terminales.

UMTS *Universal Mobile Telecommunications System*. Sistema universal de telecomunicaciones móviles de tercera generación de la ITU, sucesor del sistema GSM.

UNI *User-Network Interface*. Define la frontera del ámbito estrictamente de usuario y del ámbito de la red de acceso o servicio.

URI *Uniform Resource Identifier*. Esquema de identificación de usuario.

UTRAN *UMTS Terrestrial Radio Access*. Definición de la red radio de UMTS según el 3GPP.

VCC *Voice Call Continuity*. Habilitador de servicio definido por el 3GPP que permite la continuidad de una sesión de voz mientras el usuario se mueve de una red de acceso a otra de tecnología distinta.

WSDL *Web Services Description Language*. Lenguaje basado en XML usado para describir los servicios web que un negocio ofrece.

XCAP *XML Configuration Access Protocol*. Es un protocolo que permite a un cliente leer, escribir y modificar datos de configuración de una aplicación almacenados en un servidor en formato XML.

XML *eXtensible Markup Language*. Lenguaje de marcas desarrollado por el W3C que permite definir la gramática de lenguajes específicos para estructurar documentos grandes.

Bibliografía

ITU-T Recomendación Y.2012 (abril 2010). *Functional requirements and architecture of next generation networks*

ITU-T Recomendación Y.2111 (noviembre 2011). *Resource and admission control functions in next generation networks*

ITU-T Recomendación Y.2018 (septiembre 2009). *Mobility management and control framework and architecture within the NGN transport stratum*

3GPP Recomendación TS 23.203 v15.3.0 (junio 2018). *Policy and charging control architecture*

3GPP Recomendación TS 23.228 v15.2.0 (marzo 2018). *IP Multimedia Subsystem (IMS)*

3GPP Recomendación TS 29.214 v15.4.0 (junio 2018). *Policy and Charging Control over Rx reference point*

Hurwitz, J.; Bloor, R.; Kaufman, M.; Halper, F. (2009). *SOA For Dummies*, (2.ª ed.). 3GPP TS 23.198 V9.0.0. Open Service Access (OSA). Stage 2.

3GPP TS 23.216 v15.2.0 (2018-06) (junio 2018). *Single Radio Voice Call Continuity (SRVCC)*

3GPP TS 23.141 v15.0.0 (junio 2018). *Presence service; Architecture and functional description*

3GPP TS 24.173 v15.1.0 (junio 2018). *IMS Multimedia Telephony Communication Service and Supplementary Services*

Poikselka M.; Mayer G. (2009). *The IMS: IP multimedia concepts and services*, 3rd Ed.

Enlaces de interés:

Ejemplos de flujos de llamadas IMS:http://www.eventhelix.com/realtimemantra/telecom/

OMA Presence Simple:http://www.openmobilealliance.org/Technical/release_program/presence_simple_v1_1.aspx

SOAP:http://www.w3schools.com/soap/soap_intro.asp

WDSL:http://www.w3.org/TR/wsdl