NGN/IMS a fondo

Víctor Huertas García

PID_00175639

UOC
Universitat Oberta de Catalunya

Índice

Introducción

Un nuevo paradigma ha surgido en el mundo de las redes de telecomunicaciones y sus servicios: las redes de próxima generación o redes NGN, haciendo que cualquier red que pueda transmitir paquetes IP se convierta en una red multiservicio con garantía de calidad de servicio y no monoservicio, como sucede ahora con las redes existentes de telefonía fija/móvil. A partir de ahora los servicios ofrecidos a los usuarios y las redes de transporte ya no estarán íntimamente vinculados.

Existen muchas entidades de estandarización y especificación de todo el mundo (gubernamentales o no) que están actualmente involucradas en definir las redes NGN. Pero entre ellas hay un grupo especialmente activo en la generación de documentación, como por ejemplo, la ITU-T, la ETSI-TISPAN y sobre todo la 3GPP (entidad que ha especificado IMS).

Cada una de estas entidades da su propia versión de cómo se definen las redes NGN generando su documentación propia. Aunque en términos generales son modelos de referencia muy similares, las diferencias más importantes entre unos y otros radican en la distribución de las funcionalidades en bloques adaptándose a una tipología de red en concreto. Por ejemplo, el modelo ETSI-TISPAN se focaliza en redes fijas (xDSL) y la del 3GPP en redes móviles. La ITU-T sigue un modelo más genérico sin ninguna especialización. Hay otras entidades, quizás no tan activas en generación de documentación, que también han aportado su granito de arena, como por ejemplo, CableLabs con su modelo de referencia PacketCable 2.0, especializado en integración en NGN de redes de cable (híbrido fibra y coaxial).

Web recomendada

Más información sobre PacketCable 2.0 en: http://cablelabs.com/packetcable/specifications/specifications20.html.

Es importante que tengáis en cuenta que, a pesar de ser muy similares, estos modelos de referencia de las distintas entidades de estandarización pueden aparecer indistintamente mencionados en multitud de artículos y documentación diversa acerca de las redes NGN.

Es por ello por lo que vale la pena que seleccionemos tres modelos representativos (ITU-T, ETSI-TISPAN y 3GPP) y veamos las características más importantes de cada uno.

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 de la ITU-T, la ETSI-TISPAN y el 3GPP para las siguientes subcapas de la capa de transporte.
- Subcapa de procesado de transporte.
- Subcapa de control de transporte: adhesión a la red y control de admisión y recursos.

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

3. Para la capa de servicio, conocer los componentes del núcleo IMS para el 3GPP y las diferencias con los modelos equivalentes de la ETSI-TISPAN y la ITU-T.

4. Identificar los puntos de referencia (o interfaces) entre bloques funcionales del núcleo IMS.

5. Identificar y conocer los puntos de referencia (o interfaces) entre el núcleo IMS y la capa de transporte.

6. Identificar otros bloques funcionales en la capa de servicio que las entidades de estandarización ETSI-TISPAN y ITU-T añaden a los estrictamente definidos en el núcleo IMS y que complementan otras funcionalidades de provisión de servicio.

7. Conocer los dos mecanismos que las redes NGN definen en el proceso de reserva de recursos y garantía de QoS, en la red de transporte, durante el establecimiento de la sesión de servicio: modo *push* y modo *pull*.

8. 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.

9. Saber los pasos que un terminal tiene que dar para acceder a la red de acceso y posteriormente poder acceder a los servicios IMS.

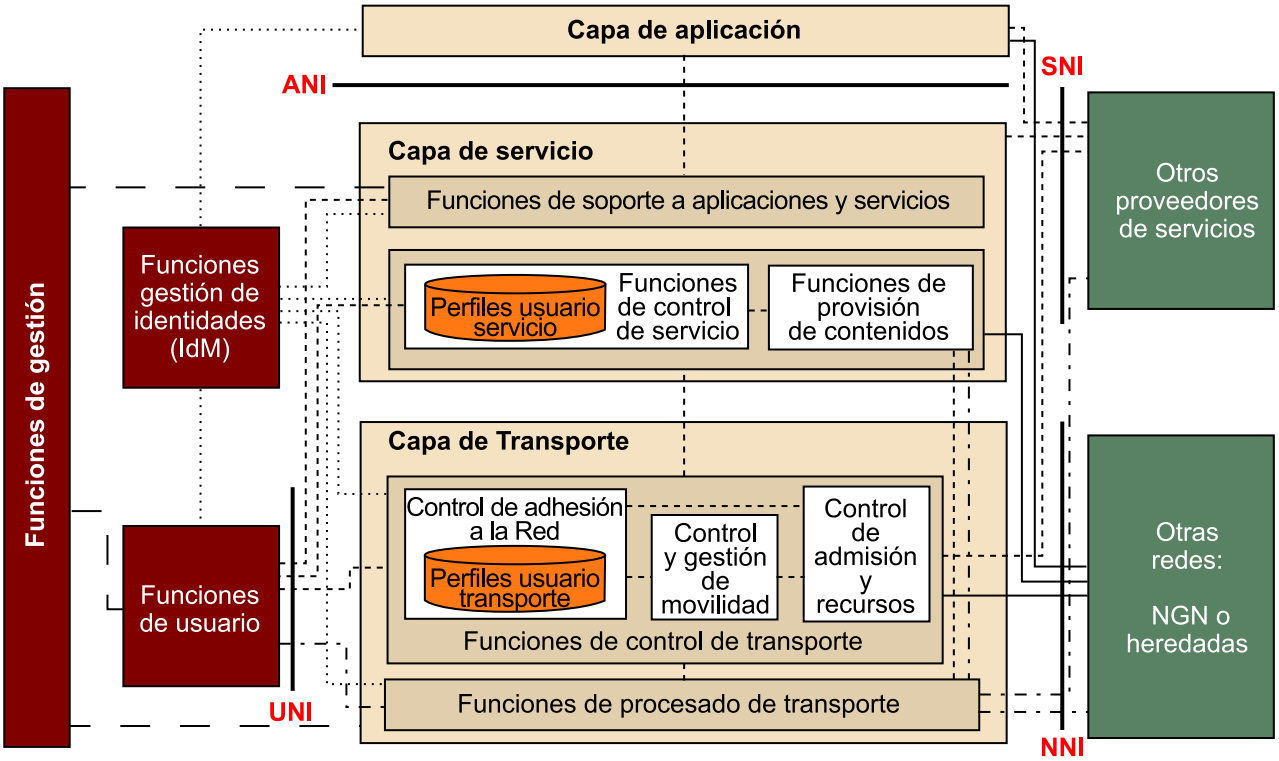
10. Conocer el flujo de llamada IMS, identificando los mensajes SIP que se intercambian para los servicios más representativos.

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).

Estas características definen una arquitectura de referencia horizontal separada en capas de transporte y servicio. En la siguiente figura, la ITU-T nos muestra su visión de dicha arquitectura.

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



La figura 1 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 continuación veremos cada una de las partes y capas que conforman la arquitectura ITU-T de referencia empezando por la capa de transporte y sus funciones, y subiendo hasta la capa de servicio. Además, para cada una de las partes, también veremos el modelo que definen otras dos de las organizaciones más activas en la tarea de generación de documentación de especificación sobre las redes NGN: la ETSI-TISPAN y el 3GPP.

Aunque el modelo de referencia de la ITU-T es el que se considera como global y armonizador de otros estándares, vale mucho la pena ver estas otras dos especificaciones, ya que es muy normal leer publicaciones con estos dos modelos. Veremos también las diferencias y similitudes entre ellos.

1.1. Elementos que definen la arquitectura

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, independientemente del modelo que describamos.

1.1.1. 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 del mismo solo tiene sentido cuando conocemos las instancias particulares que se usan en un contexto.

1.1.2. Punto de referencia

El punto de referencia o interfaz es un punto de unión entre dos entidades funcionales bien diferenciadas. Los puntos de referencias 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 y/o H.248.

1.2. Capa de Transporte

A continuación vamos a hacer un barrido por tres especificaciones de las entidades estandarizadoras más activas en especificación de redes NGN. Empezaremos por la ITU-T y luego miraremos las de la ETSI-TISPAN y 3GPP a modo de comparación con la primera.

1.2.1. Arquitectura de referencia de la ITU-T

La definición de la arquitectura de referencia de la capa de transporte para la ITU-T está dividida en dos subcapas: la de procesado y la de control. A su vez, cada subcapa está desglosada y atomizada en funciones y subfunciones. Esto es muy normal, ya que la ITU-T ejerce de entidad de estandarización global que se encarga de armonizar las aportaciones de otros estándares como la ETSI o el 3GPP, que están focalizadas a un tipo concreto de tecnología de red de acceso.

Así pues, veremos definiciones de funcionalidades genéricas que intentan huir de cualquier especificación que se decante por un tipo de tecnología de red de acceso en concreto y a la vez intentan no descartar ningún tipo de tecnología que pueda existir en este ámbito.

Subcapa de procesado de transporte

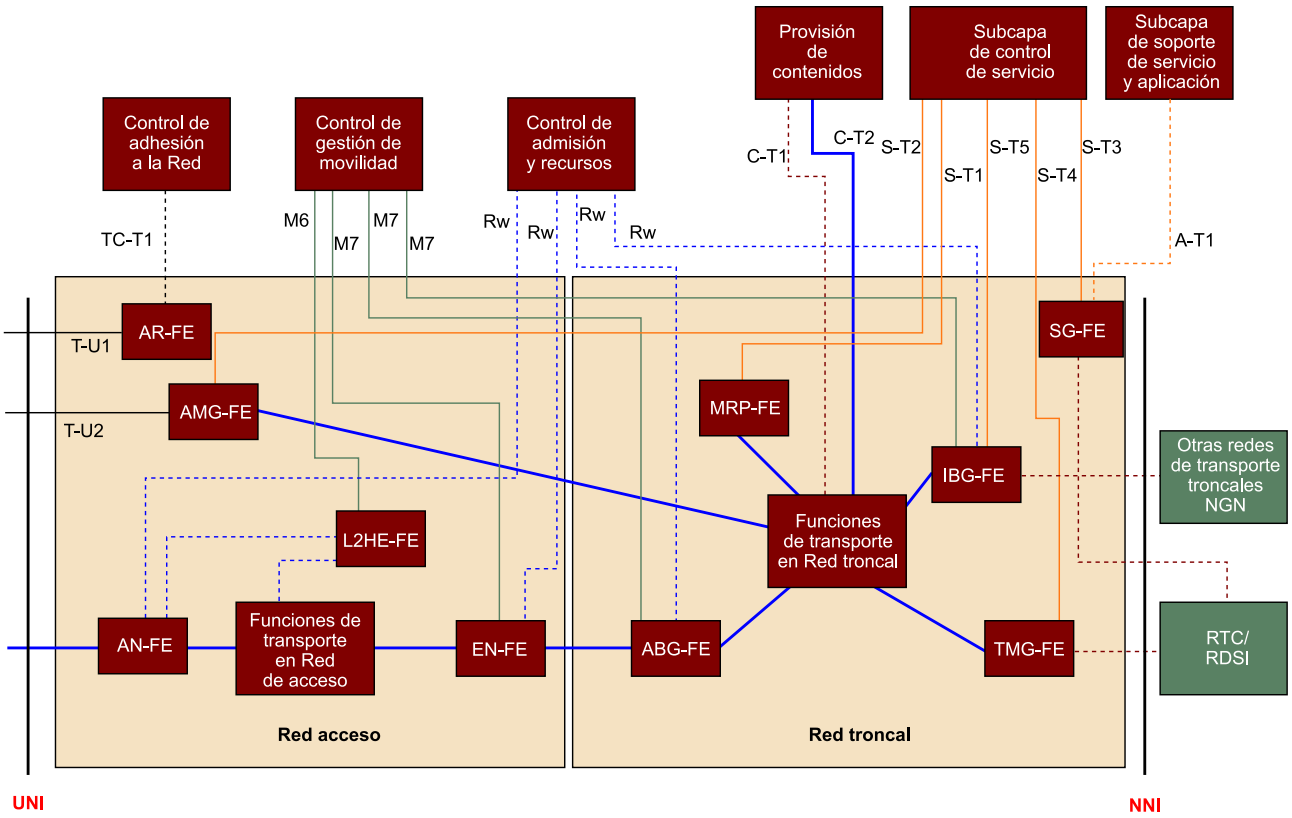
La arquitectura que la ITU-T propone de entidades funcionales para la subcapa de procesado de tráfico en la capa de transporte se puede apreciar en la figura 2. Las entidades funcionales de esta subcapa están clasificadas en dos secciones:

- red de acceso y
- red troncal.

Red de acceso y red troncal

Dentro de las redes de transporte, la red de acceso se considera la última milla antes de llegar al terminal de usuario, y la red troncal es la red de alta capacidad que interconecta varias redes de acceso entre sí.

Figura 2. Entidades funcionales y puntos de referencia para capa de procesado de transporte



A continuación veremos qué funcionalidades tiene cada entidad y los puntos de referencia que las unen. Empezaremos definiendo algunas entidades funcionales elementales que pueden estar presentes en una o más entidades que aparecen en la figura 2, y seguidamente abordaremos las entidades propias de la red de acceso y de la red troncal.

1) Entidades elementales de procesado de transporte

Las entidades elementales no toman decisiones por sí solas sino que son controladas por otras entidades de control (localizadas en la subcapa de control de transporte o de control de servicio) con el objetivo de garantizar la QoS de los servicios.

a) Entidad Funcional de Aplicación de Políticas (PE-FE): Esta entidad se hace llamar en inglés Policy Enforcement Functional Entity y posee los mecanismos necesarios para aplicar políticas concretas de procesado de paquetes IP. Entre estos mecanismos están el filtrado, clasificación y marcado de paquetes, conformación de tráfico a nivel de flujo o de usuario así como gestión de colas, y priorización.

Dichas políticas a ejecutar son decididas y especificadas por otra entidad llamada *PD-FE* (Policy Decision Functional Entity) localizada en la subcapa de control de transporte, como veréis más adelante.

Veréis posteriormente que el lugar típico donde se integra esta entidad funcional es donde hay potencialidad de producirse un cuello de botella en términos de capacidad, o también donde se requiere hacer un control de los recursos de transporte.

Recurso de transporte

El concepto de recurso de transporte no solo incluye el concepto de ancho de banda o capacidad en bits por segundo, sino también en el ámbito de la traducción de direcciones IP o puertos. En IPv4 la cantidad de direcciones IP públicas es un recurso finito y por lo tanto a controlar.

Un ejemplo de estos lugares son las pasarelas a nivel de paquete IP que están en los límites de la red de acceso o en las funciones de usuario.

b) Entidad Funcional de Aplicación de Recursos de Transporte (TRE-FE): Esta entidad, que en inglés se traduce como Transport Resource Enforcement Functional Entity, depende de la tecnología asociada al segmento de la red de acceso que controla y aplica políticas de recursos de transporte especificadas por la entidad de control respectiva (TRC-FE, en la subcapa de control de transporte).

En una red TDMA, el TRE-FE sería el bloque que asigna dinámicamente los *slots* a cada terminal de usuario para cumplir con una capacidad de transmisión determinada por el gestor de recursos (TRF-FE).

c) Entidad Funcional de Transferencia Elemental (EF-FE): En inglés se traduce como Elementary Forwarding Functional Entity y se puede definir como un elemento físico que transfiere un paquete de datos desde una interfaz de entrada a otra interfaz de salida. La ITU-T llama a esta interfaz Flow Point (FP).

Unicast y multicast

Si el paquete se transmite en *unicast*, éste entra por un solo FP y sale por otro de salida (diferente al de entrada). Si la transferencia es *multicast*, el paquete entra por un solo FP de entrada y sale por ninguno o varios FP de salida (nunca por el mismo FP de entrada).

La entidad EF-FE es controlada por su entidad correspondiente de control (EC-FE), que es la que le indica por qué FP debe sacar los paquetes en función de parámetros del propio paquete recibido.

Un ejemplo claro de esta funcionalidad es la que contiene un encaminador (capa 3) cuando aplica rutas IP configuradas, o un *switch* (capa 2) cuando consulta la tabla MAC.

d) Entidad Funcional de Control Elemental (EC-FE): En inglés se llama Elementary Control Functional Entity y se encarga de procesar datos de control de protocolos tanto para *unicast* como para *multicast*, de cara a configurar el comportamiento del EF-FE. También puede recibir peticiones desde el TRE-FE y el PE-FE para la aplicación de políticas y responderles sobre el resultado de dicha operación.

Ejemplos de esta entidad funcional son la capacidad de procesado de paquetes de enrutamiento dinámico (RIP, OSPF, etc.) de un encaminador (capa 3) o de Spanning Tree en el caso de un *switch* (capa 2). Otro ejemplo sería que el EC-FE fuera una aplicación externa que configurara de manera estática las rutas IP en función de criterios arbitrarios de operador.

2) Entidades funcionales de procesado de transporte en la red de acceso

Recordemos que la red de acceso lo forman entidades funcionales que interactúan directamente con el terminal de usuario. Se asume que la red de acceso NGN es una red que es capaz de transmitir paquetes IP. La ITU-T intenta copar cualquier terminal con tecnología de red existente, incluyendo las de redes heredadas que no están diseñadas para la transmisión de paquetes IP. Como veremos a continuación, habrá entidades funcionales que deberán soportar interconexión con este tipo de tecnologías.

Veamos pues las cinco entidades funcionales de procesado de transporte en la red de acceso. Son las siguientes:

a) Pasarela de Medios de Red de Acceso (AMG-FE): En inglés responde a las siglas de *Access Media Gateway Functional* Entity y básicamente se encarga de interconectar la red de acceso para transporte de paquetes IP con terminales de usuario basados en líneas telefónicas analógicas o de RDSI. Esta entidad está controlada por otra entidad funcional situada en la subcapa de control de servicio, llamada Pasarela de Control de Señalización (AGC-FE, con sus siglas en inglés). Este control se establece a través de un punto de referencia llamado T-U2.

RTC /RDSI (conmutación de circuitos) e IP son tecnologías radicalmente distintas y de aquí se extraen las siguientes subfunciones:

Nota

La recomendación ITU-T Y.1453 especifica la interconexión entre interfaces RDSI e IP.

- Procesamiento bidireccional de medios en el plano de usuario (flujos de tráfico de voz, básicamente) entre la tecnología RTC/RDSI y la red NGN. Opcionalmente, se incluyen funciones como la transcodificación y la cancelación de eco (caso de un terminal de usuario con línea analógica). También puede realizar funciones de interactividad entre el sistema TDM e IP para soportar servicios de emulación RDSI en casos en que se necesite un enlace RDSI sin restricciones.

- Reenvío de la señalización de control de llamada de un usuario de la tecnología RTC/RDSI hacia la AGC-FE. Implica una traducción de los mensajes de señalización a su equivalente en IP (normalmente a SIP).

  Un ejemplo claro de implementación en la vida real de esta entidad funcional es una Gateway de VoIP, que tiene una o varias interfaces RDSI y por otro lado una interfaz IP por la que procesa la señalización SIP o H.323 y los flujos RTP donde va la carga útil.

b) Nodo de Acceso (AN-FE): En inglés Access Node Functional Entity, es el punto de terminación o inicio del último tramo de la red de acceso antes de llegar justo a las entidades funcionales de las funciones de usuario (ver la figura 1). Dependiendo de la arquitectura y la tecnología de la red de acceso, este bloque puede que no esté presente. Pero si lo está, por norma general se trata de un elemento de capa 2 (enlace)y que opcionalmente puede soportar capa 3 (IP). Así, el AN-FE es un elemento con potencialidad de cuello de botella y, por lo tanto, tiene que soportar las funciones de control dinámico de calidad de servicio ejecutadas por las entidades EC-FE, EF-FE, PE-FE y TRE-FE, y definidas por las entidades funcionales de la subcapa de control de transporte para tal función como del bloque de control de admisión y recursos (RACF). La comunicación entre ambos grupos de bloques se realiza vía una interfaz llamada Rw.

Nota

Estas funciones de control de QoS son realmente necesarias cuando esta entidad funcional soporta la capa IP.

c) Nodo Fronterizo (EN-FE): Llamado en inglés Edge Node Funcional Entity realiza las funciones de nodo frontera entre el ámbito de la red de acceso y la red troncal de transporte. Puesto que la red troncal de transporte soporta obligatoriamente la capa 3 (IP), esta entidad funcional se puede considerar como el nodo en que termina la sesión de capa 2 (enlace entre el terminal de usuario y la red de acceso) y donde empieza la red puramente IP (siempre que el nodo de acceso no soporte capa IP). Esto conlleva la posibilidad de ser cuello de botella, con lo cual, a parte de las funcionalidades de transferencia de paquetes descritas ya como la EF-FE y la EC-FE, puede albergar también las funciones de priorización y control de recursos descritas en las entidades elementales de aplicación de recursos de transporte y de políticas (TRE-FE y PE-FE). Dichas funciones también serían controladas por el RACF vía la interfaz Rw.

Nota

En redes de acceso móviles, el EN-FE puede incluir funcionalidades de ejecución de *handover* en capa 3. El *handover* en capa 3 se dispara cuando el terminal de usuario sale del ámbito de la subred de acceso en la que se encuentra y se desplaza a otra subred que requiere el cambio de asignación de dirección IP. Con la definición de un nodo fronterizo con capacidad opcional de ejecución de *handover* en capa 3, la ITU-T deja la puerta abierta a las redes de acceso móviles. Las funciones de movilidad descritas por la ITU-T se describen con más detalle en el documento ITU-T Y.2018.

d) Entidad Funcional de Retransmisión de Acceso (AR-FE): En inglés se traduce a Access Relay Functional Entity. Esta entidad no procesa paquetes de tráfico del usuario sino que se involucra en procesos de ingreso en la red de los terminales de usuario recibiendo solicitudes de estos (a través de una interfaz llamada T-U1) y transfiriéndolos directamente al bloque AM-FE (Access Management Funcional Entity) dentro del Control de Adhesión a la Red (NACF), vía un punto de referencia llamado TC-T1. En dicha transferencia, el AR-FE puede añadir información de configuración local que pueda creer conveniente para el NACF.

Ingreso en la red de acceso

Ingreso en la red de acceso se entiende como autenticación mutua entre el terminal de usuario y la red y posterior asignación de dirección IP dentro del ámbito de la red de acceso. Es el primer paso que todo terminal de usuario debe realizar antes de poder acceder a ningún servicio contratado a través de una red de acceso.

Por ejemplo, imaginemos que en un caso real la sesión de capa 2 entre el terminal de usuario y la red de acceso está basada en el protocolo PPP. Con el establecimiento de conexión que define este protocolo se puede autenticar el terminal de usuario y asignar dinámicamente una dirección IP. Entonces el AR-FE actuaría como un reenviador de PPPoE (encapsulación de tramas PPP en una trama Ethernet) hacia el NACF.

En cambio, si se usa DHCP, el AR-FE actuaría a modo de reenvío de los paquetes DHCP al NACF. Además podría añadir información a dicho mensaje DHCP antes de reenviarlo, informando sobre el identificador de canal virtual asociado (en el caso de que fuera una red ATM).

e) Entidad Funcional de Ejecución de Handover en capa 2 (L2HE-FE): El Layer 2 Handover Execution Functional Entity está claramente orientada a redes con movilidad (inalámbricas) en los que el terminal de usuario se desplaza de una celda de cobertura a otra. Básicamente, aplica mecanismos asociados a la movilidad en la capa de enlace (no en capa IP) para preservar la continuidad del flujo de datos en el proceso de *handover*. Estos mecanismos están controlados por el bloque de control de movilidad llamada *MMCF* (Mobility Management Control Function) en la subcapa de Control de Transporte. Dentro de este bloque es la entidad HDC-FE (Handover Decision Control Functional Entity), vía una interfaz llamada M6, que toma las decisiones del proceso de *handover* de un equipo de usuario en la red de acceso. El L2HE-FE intercambia con esta entidad eventos y acciones para garantizar la continuidad del flujo de datos. Como es de suponer, este proceso está muy ligado a la tecnología y la tipología de la red de acceso.

Nota

La ITU-T no ha definido una entidad funcional separada a la equivalente en capa 3. Directamente está integrada en otras entidades, como ya hemos visto. Para una información más detallada sobre los mecanismos que la ITU-T define para *handover* de capa *2 y* capa 3, consultad la recomendación Y.2018.

3) Entidades funcionales de procesado de transporte en la red troncal

A continuación pasamos la frontera de la red de acceso (considerada como la última milla antes del terminal de usuario) y nos pasamos a una red aglutinadora de tráfico que viene desde o va hacia las redes de acceso. Aquí las redes troncales ya se consideran puramente NGN y, por lo tanto, todas las entidades soportan la transferencia de paquetes IP. En este ámbito, se presentan las cinco entidades funcionales que conforman el procesado de transporte en la red troncal:

a) Pasarela Fronteriza de la Red de Acceso (ABG-FE): el Access Border Gateway Funcional Entity es el elemento 'espejo' del nodo fronterizo EN-FE en la red de acceso, ya que simplemente realiza transferencias de paquetes IP entre los segmentos de red de acceso y troncal (esto es lo mismo que decir que incluyen las funcionalidades elementales de transferencia de paquetes como EF-FE y EC-FE). Como la red troncal y la de acceso pueden pertenecer a dominios administrativos distintos (operadores distintos), esta entidad puede realizar otras funciones fronterizas (protección mutua mediante ocultación o enmascaramiento de la tipología de red).

Es importante mencionar que, al ser un elemento fronterizo de transferencia de paquetes IP entre dos ámbitos distintos de la red de transporte, opcionalmente el ABG-FE puede soportar la traducción de direcciones IPv4 a IPv6.

Enmascaramiento

Cuando decimos enmascaramiento queremos decir que, por ejemplo, se incluyen funcionalidades como apertura o cierre de puertas de acceso a nivel de flujo IP o filtrado de paquetes a modo de cortafuegos. También sería capaz de realizar traducción de direccionamiento tanto a nivel de dirección IP como a nivel de puerto (NAPT), aplicada a flujos multimedia (llamado *media latching*). La configuración de dichas traducciones puede ser controlada remotamente por entidades en la subcapa de Control de Transporte (el RACF vía la interfaz Rw), y para que tal control se lleve a cabo el ABG-FE debe implementar parte de las funciones elementales de aplicación políticas descritas anteriormente en la PE-FE, en concreto, la conformación de tráfico y el remarcado de paquetes.

Puede parecer absurdo tener dos entidades adyacentes que realizan prácticamente la misma función, pero es muy importante de cara a delimitar dos dominios administrativos distintos, que son operados por dos organizaciones completamente distintas. Es pues deseable y lógico que ambos operadores se protejan de algún modo haciendo que la única entidad visible de cada red operada por entidades externas sea un único elemento. Así, pueden controlar mucho mejor el tráfico entrante desde otras redes externas.

Al igual que en el elemento EN-FE, esta entidad podría tener opcionalmente integrada la funcionalidad de ejecución de *handover* en capa 3 (L3HEF). De ahí que se haya dibujado la interfaz M7 en la figura 2.

b) Pasarela de Interconexión Fronteriza (IBG-FE): En inglés se define como Interconnection Border Gateway Functional Entity y es el elemento que marca la frontera entre la red troncal NGN (red de paquetes de alta capacidad) con otra red troncal NGN de las mismas características pero de otro operador. Sería el equivalente en funciones a la pasarela ABG-FE (control dinámico de QoS, traducción de direccionamiento y cortafuegos) pero en el otro extremo de la red troncal.

Como opción, esta entidad fronteriza contempla también otras funciones más complejas que dependerán del servicio, como por ejemplo, la transcodificación de medios para el servicio de VoIP, la traducción de direcciones IPv4 a IPv6 o el cifrado de medios entre otras funciones.

Al igual que con el ABG-FE, se contempla la posibilidad de integrar funcionalidades de movilidad en capa 3 en esta entidad (L3HEF). De ahí que se haya incluido la interfaz M7.

IBG-FE

Al ser la IBG -FE una entidad fronteriza entre dos dominios administrativos independientes, surge de nuevo la necesidad de protegerse que ya hemos comentado en el caso de la pasarela fronteriza de la red de acceso. Controlado por un RACF vía la interfaz Rw, la pasarela IBG-FE implementaría las funciones básicas de aplicación de políticas de la entidad elemental PE-FE (con excepción de las funciones para atravesar la traducción de dirección IP privada a pública y puertos, ya que no existen en el IBG-FE) y las de aplicación de recursos de transporte del TRE-FE. Se recomienda además soportar las funciones elementales de transmisión de paquetes EC-FE y EF-FE.

Nota

La ITU-T ya contempla que un RACF esté dedicado exclusivamente a controlar el IBG-FE dentro de una red troncal. No obstante, también contempla que otra entidad funcional distinta controle el IBG-FE: el IBC-FE o Interconnection Border Control Functional Entity, pero la especificación de su integración está bajo estudio por la ITU-T.

Tenemos que imaginarnos que habrá tantas instancias del IBG-FE como número de interconexiones haya con otras redes troncales operadas por terceros.

c) Pasarela de Medios hacia Redes de Circuitos (TMG-FE): En inglés se traduce como Trunking Media Gateway Functional Entity. Así como la pasarela fronteriza de la red de acceso (AMG-FE) que hemos visto antes ejercía la función de pasarela entre la tecnología RTC/RDSI y la red IP de cara a terminales de usuario telefónicos, esta entidad hace la misma función pero en la red troncal (incluyendo funciones de transcodificación, cancelación de eco y punto de conferencia). Es decir, que proporciona a las redes NGN (basadas en paquetes IP) la interconexión con las redes tradicionales de telefonía RTC o RDSI. Esta entidad, como la AMG-FE, tiene su entidad homóloga a nivel de control y se trata de la MGC-FE (Media Gateway Control Functional Entity) localizada en la subcapa de control de servicio. De ahí que se haya incluido la interfaz llamada S-T4.

Nota

Esta entidad proporciona la interconexión de las redes NGN con terceros operadores de redes tradicionales. La ITU-T contempla, como es lógico, interconectar los servicios de voz de NGN con dichas redes para garantizar la máxima interoperabilidad e interconectividad de todas las tecnologías.

d) Entidad Funcional de Procesado de Recursos de Medios (MRP-FE): También llamada en inglés Media Resource Processing Functional Entity, esta entidad funcional proporciona procesado de la carga útil de paquetes usados en la red troncal NGN. Esta entidad aparece como una fuente de recursos adicionales que enriquecen el servicio de llamada de voz. Por enriquecimiento nos referimos a todas aquellas funciones que hacen que el servicio de voz vaya más allá de una mera llamada entre dos terminales. Por ejemplo, generación de tonos (de espera, comunicando, etc.), generación y recepción de tonos DTMF, generación de locuciones o avisos de voz automática, transcodificación (descodificar y codificar de nuevo con otro codificador de voz), reconocimiento de voz y mezclado de vídeo u otros medios entre sí. Todas estas funcionalidades son decididas y controladas por otra entidad de la capa de control de servicio llamado Media Resource Control Functional Entity vía de una interfaz llamada S-T1.

Reflexión

Pensad que toda la señalización acústica en el mundo de la telefonía que nosotros como usuarios reconocemos enseguida (como, por ejemplo, el tono de comunicando o los mensajes de la operadora indicando que el número no está accesible), han de ser trasladados al mundo IP, y eso conlleva que alguna entidad se encargue de generar los flujos RTP de audio que un terminal de VoIP soporte y convierta a señal acústica. La ITU-T ha querido separar todos estos servicios en un elemento independiente como la MRP-FE.

e) Pasarela de Señalización (SG-FE): En inglés, la entidad se llama Signalling Gateway Functional Entity y se encarga simplemente de traducir los mensajes de señalización entre la red NGN y las redes heredadas, como la RTC, RDSI y las redes basadas en SS7. Dicha señalización en el lado NGN se reenvía a la misma entidad de control asociada a la pasarela de medios TMG-FE (la entidad de control de pasarelas de medios o MGC-FE que está localizada en la capa de control de servicio). La MGC-FE se encarga de encaminar dicha señalización hacia las funciones de encaminamiento de señalización NGN adecuadas dentro de la capa de control de servicio (la señalización en NGN en este caso sería SIP).

Reflexión

Tal y como está formada una pasarela de VoIP, no sería descabellado pensar que la SG-FE estuviera integrada con la TMG-FE en un mismo equipo físico. De hecho se podría decir que la suma de SG-FE y TMG-FE sería el equivalente a la AMG-FE pero en la red troncal. La posible razón por la que la ITU-T ha separado la señalización y el procesado de los medios en dos entidades independientes es la mayor complejidad y variación en la señalización de la red troncal de telefonía en comparación con la AMG-FE.

Subcapa de control de transporte

En la subcapa de control de transporte radica la inteligencia de gestión de recursos tanto de la red de acceso como de la red troncal. Además, esta subcapa es de suma importancia, ya que, gracias a los puntos de referencia abiertos que les conectan con la capa de servicio, proporcionan en cierta manera la independencia entre la tecnología de la red de transporte y los servicios, garantizando, si es necesario, la QoS extremo a extremo. Esta subcapa está formada por tres bloques principales: el de control de adhesión a la red (NACF en sus siglas en inglés), el de control de admisión y recursos (RACF) y finalmente el de control de gestión de movilidad(MMCF). Para cada uno de estos bloques describiremos su arquitectura y funciones.

1) Control de adhesión a la red (NACF)

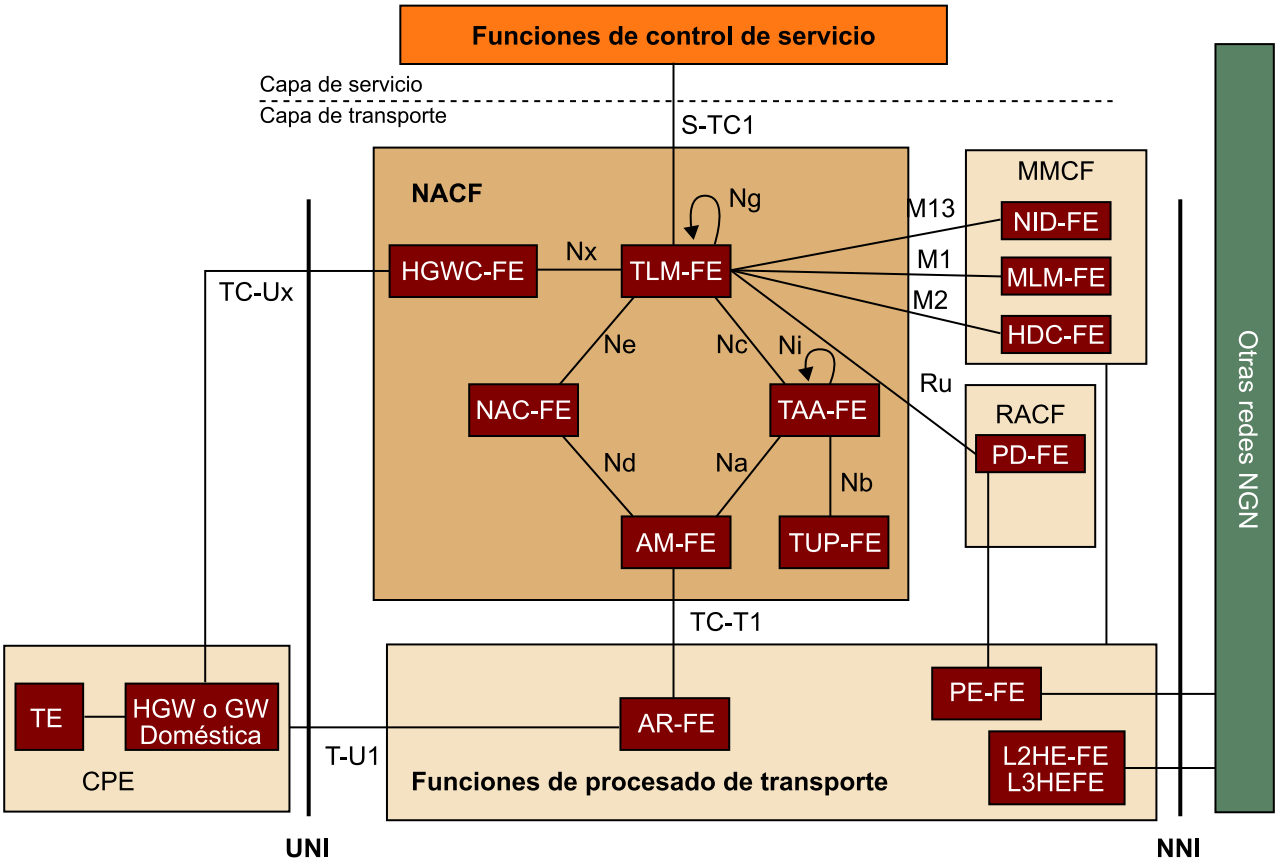
A continuación veremos las recomendaciones de la ITU-T para realizar un correcto ingreso de un terminal o equipo de usuario en la red de acceso. Este proceso es siempre el preludio para poder acceder a los servicios que ofrece una red NGN.

A continuación veremos una descripción de cada entidad funcional y cómo está relacionada con sus adyacentes.

Ved también

En la tabla 4 del anexo, podemos ver los puntos de referencia que afectan al NACF.

Figura 3. Arquitectura de referencia del NACF para la ITU-T



a) Entidad Funcional de Configuración de Acceso a la Red (NAC-FE): El Network Access Configuration Functional Entity, en inglés, se responsabiliza de la asignación de la dirección IP al equipo de usuario (al equipo de usuario en inglés también se le llama *Customer Premises Equipment* o CPE) una vez este se ha autenticado contra la entidad encargada de la autenticación y autorización a nivel de transporte (TAA-FE).

El NAC-FE puede asignar dos IP a un equipo para soportar movilidad IP: una IP persistente, que nunca varía, y una IP temporal que va cambiando cada vez que el usuario cambia de subred.

Nota

No hay una única manera de implementar esta entidad funcional. Recordad que las entidades funcionales describen meras funcionalidades pero no maneras de llevarlas a cabo. Para implementar el NAC-FE, quizás la primera idea que os viene es utilizar un servidor DHCP, pero también se podría implementar con un servidor PPP que haga la misma función. En definitiva, como cualquier otra entidad funcional descrita en este documento, hay total libertad en la implementación del NAC-FE siempre que cumpla cada una de las funcionalidades descritas.

Aparte de asignar la dirección IP, el NAC-FE puede aprovechar esta transacción para distribuir otros parámetros de configuración de red como las direcciones de servidores DNS o las de *proxies* de señalización para algunos componentes de la capa de servicio (como por ejemplo, el P-CSC-FE que el punto de presencia del núcleo IMS para el usuario en la capa de control de servicio).

Nota

También se puede contemplar la posibilidad de que esta información adicional de configuración de red (*DNS*, *proxies*) esté estáticamente configurada en el equipo de usuario, inclusive la asignación estática de la dirección IP (si el perfil de usuario a nivel de transporte así lo indica).

Situándonos en un escenario de itinerancia del equipo de usuario (es decir, que ingresa en una red de acceso de otro operador), esta entidad funcional puede estar localizada en una red visitada o en una red local dependiendo del dominio administrativo y del escenario de negocio.

b) Entidad Funcional de Autenticación y Autorización a Nivel de Transporte (TAA-FE): El Transport Authentication and Authorization Functional Entity realiza la autenticación del usuario así como el control de autorización basada en perfiles de suscriptor a nivel de transporte, de cara al acceso a la red. Esta funcionalidad es siempre previa a la asignación de la dirección IP por el NAC-FE.

Para poder autenticar y autorizar al usuario, el TAA-FE necesita información sobre las credenciales y del perfil de suscripción del mismo. Esta información la proporciona otra entidad funcional dentro del NACF llamada *TUP-FE* y que más tarde se va a detallar.

En un escenario de itinerancia de ingreso en la red, el TAA-FE puede realizar el papel de proxy para conectarse a otra entidad TAA-FE remota donde se encuentra la información de autenticación almacenada del usuario en cuestión (en el TUP-FE correspondiente). Para ello se requiere del punto de referencia Ni.

En el proceso de adhesión a las redes NGN, se contemplan dos métodos de autenticación:

- La **autenticación implícita**, en el que simplemente con la consulta de un parámetro que identifique unívocamente al equipo de usuario (por ejemplo, una dirección MAC en una lista de admitidos) pueda ser suficiente.
- La **autenticación explícita**, en el que lanza un reto al equipo de usuario y se desencadena el procedimiento de autenticación por mecanismos y protocolos de comprobación de credenciales.

c) Entidad Funcional de Perfil de Usuario a Nivel de Transporte (TUP-FE): El Transport User Profile Functional Entity es la entidad funcional a modo de base de datos que almacena en un mismo perfil lo siguiente:

- **Datos de autenticación**: entre los que se incluyen: 1) el identificador de suscriptor a nivel de capa de transporte, 2) la lista de métodos de autenticación soportados o 3) las claves a usar.

- **El perfil de suscripción de transporte**. Este contiene la información relacionada con la configuración requerida para el acceso a la red, así como la información de perfil de QoS contratado por el usuario en el ámbito de la red de acceso.

Al igual que en el caso de la entidad que asigna el direccionamiento IP (NAC-FE) para el escenario de itinerancia, la información puede ser transferida a un TUP-FE de una red visitada, pero siempre a través de la entidad TAA-FE. Es decir, que la capacidad de transferencia de perfiles la tiene realmente el TAA-FE, el cual tiene un punto de referencia específico (llamado Nb) para esta función.

Información TUP-FE

Es posible que os hagáis la pregunta sobre qué formato o información exacta contienen estos perfiles. La ITU-T ya especifica en su recomendación Y.2014, donde describe con detalle el bloque NACF de adhesión a la red de transporte y todos sus bloques funcionales, una tabla en la que indica qué parámetros define dicho perfil. A modo de resumen, cada perfil de transporte tiene su identificador único conteniendo información de acceso a la red. Pero asociado a éste, existen varios subperfiles, cada uno con su propio identificador, todos ellos con información de autenticación y perfil de recursos de transporte propios. Este identificador de subperfil es el identificador que se corresponde con otro identificador de conexión lógica en la red de acceso (equivalente por ejemplo a ID de canal virtual en ATM o a la etiqueta asignada en una red MPLS).

d) Entidad Funcional de Gestión de Localización a Nivel de Transporte (TLM-FE): El Transport Location Management Functional Entity registra la asociación entre la dirección IP asignada a un equipo de usuario y la información de localización en red relacionada con el mismo, la cual es proporcionada por la entidad NAC-FE vía la interfaz Ne.

Ejemplo

Esta información de localización en red incluye, por ejemplo, características del equipo en la red de acceso, un identificador de conexión lógica (es un identificador que define la conexión o canal virtual que lleva al acceso directo del equipo de usuario) o la identificación del equipo limítrofe en la central que cierra el bucle de abonado (algo típico en redes ADSL).

El TLM-FE registra también la asociación entre la información de localización a nivel de transporte recibida desde la entidad funcional NAC-FE y la información de localización geográfica (en forma de coordenadas o incluso su dirección postal). Además, añade a esta asociación el perfil de QoS del usuario recibido desde TAA-FE, vía la interfaz llamada Nc, para luego pasárselo al RACF (Control de Admisión y Recursos) vía la interfaz llamada Ru. Más tarde se verá para qué el RACF usa esta información.

Información geográfica

La capa de control de servicio solicita la información geográfica (coordenadas de localización) a través de un punto de referencia llamado S-TC1. Sin embargo, el estándar de la ITU-T no especifica cómo el TLM-FE obtiene dicha información geográfica. Esta infor-

mación, al ser en determinados casos delicada para el usuario, puede restringirse o no mostrarse deliberadamente si éste así lo acuerda con el operador de red de acceso.

e) Entidad Funcional de Gestión a Nivel de Acceso (AM-FE): El Access Management Functional Entity, como se llama en inglés, es la entidad funcional que está directamente conectada a la entidad funcional de retransmisión de acceso (AR-FE) en la subcapa de procesado de transporte vía la interfaz TC-T1. Su función es terminar a nivel de capa 2 (cuyos mensajes son recibidos desde el AR-FE) la conexión entre el equipo de usuario y el NACF de cara al registro y la inicialización del equipo de usuario. Dicha conexión de capa 2 puede ser utilizada para detectar intentos de adhesión a la red de un equipo de usuario. En este caso, la conexión de capa 2 entre el equipo de usuario y el AM-FE puede constituir un marco unificado para las entidades de capas superiores a través de entornos con redes heterogéneas para facilitar la selección y el descubrimiento de múltiples tipos de redes de acceso existentes dentro de un área geográfica. Gracias a esta conexión, el AM-FE puede descubrir los identificadores de enlace (de la conexión lógica y física).

Conexión lógica y física

Como conexión lógica lo consideramos como un identificador de canal virtual y como conexión física, algún parámetro que identifique al terminal de usuario en la red de acceso (por ejemplo, una dirección MAC, la dirección IP del elemento PE-FE asociado o un identificador de puerto físico).

Hay que clarificar que cada relación a nivel de comunicación entre el equipo de usuario y el AM-FE no implica ningún mecanismo de transporte en particular.

Ejemplo

Para entender exactamente qué papel puede jugar el AM-FE, pongamos un ejemplo. Imaginaos que el protocolo de capa 2 en la red de acceso es el PPP. Así pues, el AM-FE haría la función de servidor PPP y traduciría las peticiones de dicho protocolo a nivel de autenticación y solicitud de dirección IP a otro protocolo (RADIUS en modo cliente) a través del punto de referencia que le conecta con las entidades del NACF correspondientes (TAA-FE para autenticación y NAC-FE para asignación de dirección IP).

Otro ejemplo sería la utilización del protocolo 802.1X en el que el AM-FE haría de autenticador implementando un cliente RADIUS hacia el TAA-FE y el NAC-FE).

f) Entidad Funcional de Configuración de Pasarela Doméstica (HGWC-FE): El Home Gateway Configuration Functional Entity se usa en la inicialización y actualización remota de la pasarela doméstica (por ejemplo, instalación remota de nueva versión del *firmware*). Proporciona a dicha pasarela información de configuración adicional a nivel de cortafuegos local o marcado de paquetes para QoS (esta información puede estar almacenada en forma de perfiles de configuración en la propia pasarela doméstica) que puede ser usada en posteriores procesos de garantía de QoS (proporcionados por interacciones con el RACF a través de otras entidades funcionales). Hay que clarificar que dichos datos de configuración de red no tienen nada que ver con la configuración de red proporcionada por el NAC-FE (información de proxies, servidores DNS, etc.).

Nota

La definición del equipo de usuario por la ITU-T (o CPE, en inglés) no se ciñe solamente a un terminal único (un solo dispositivo físico) como sería el caso de un terminal de telefonía móvil, sino que el estándar también considera que el CPE pueda ser una red entera con una pasarela residencial encabezándola como, por ejemplo, el encaminador ADSL en un hogar que da servicio a toda una red detrás.

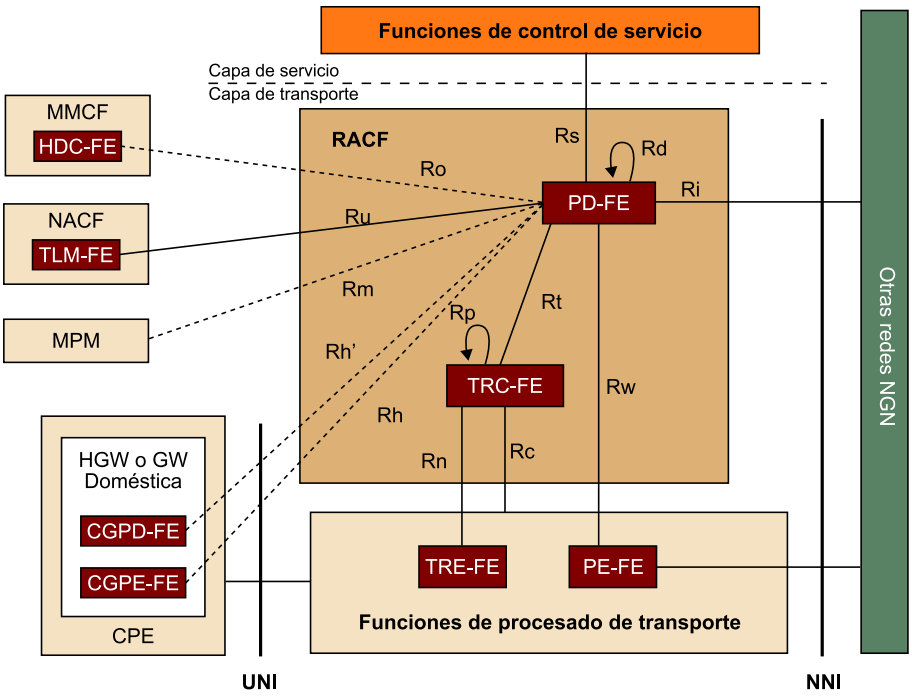
La HGWC-FE también puede gestionar información de monitorización que la pasarela doméstica pueda generar acerca de los terminales o dispositivos que tras ella se conectan (por ejemplo, sobre la disponibilidad de los equipos terminales o TE en inglés).

Esta entidad puede estar interconectada con la entidad TLM-FE para obtener información sobre el tipo de conexión o identificadores de enlace que pueda ayudarle a seleccionar la configuración más adecuada.

2) Control de Admisión y Recursos (RACF)

En la figura 4 podéis apreciar la arquitectura de referencia que la ITU-T presenta para el RACF. Como veréis a continuación, esta entidad es clave, ya que garantiza la gestión de recursos y la QoS de los servicios en la red de transporte (de acceso y troncal). Por eso vamos a dar una explicación un poco más detallada.

Figura 4. Arquitectura de referencia del RACF para la ITU-T



Antes de abordar cada uno de los bloques funcionales e interfaces que componen el RACF, vamos a definir las fases que se contemplan en el proceso de control de admisión y recursos ya que es algo común en las redes NGN.

Ved también

Sobre los bloques funcionales e interfaces del RACF, ver el resumen en la tabla 5 en el anexo.

Hay tres pasos principales en la garantía de QoS en el momento en que el RACF recibe una solicitud al respecto:

- **Autorizar** (*Authorization*). La solicitud de QoS aplicando políticas de red definidas por el operador.

- **Reservar** (*Reserve*). Los recursos en la red de transporte. En este caso se realiza una comprobación de cumplimiento de perfil de usuario (solo en caso de red de acceso) y posteriormente, una comprobación de disponibilidad de recursos en el sistema antes de hacer la reserva. Si los controles se pasan satisfactoriamente, se actualiza el estado de los recursos como reservados (pero el usuario aún no los puede usar).

- **Asignar** (*Commit*). Los recursos ya previamente reservados al usuario para que haga uso de ellos (no requiere actualización de estado de los recursos sino un asignación de estos al terminal tras el cual está el usuario).

Estos tres pasos pueden realizarse en una sola fase (bajo una sola solicitud), en una fase separada para cada paso (con tres solicitudes separadas) o en dos fases, en el que la autorización y la reserva de recursos se realiza en una sola fase y la asignación se realiza *a posteriori*, bajo sendas solicitudes de recursos desde la capa de control de servicio.

Reserva en dos fases

¿Por qué se habilita la posibilidad de realizar la reserva en dos fases? Se hace así para evitar que se asignen recursos en pleno establecimiento de la sesión de servicio y por algún motivo se cancele dicho establecimiento sin llegar a usar el servicio. Solo se asignarán los recursos cuando el establecimiento de la sesión esté totalmente asegurado y confirmado por parte de los usuarios. Además, pensad que cuando se reservan los recursos, mientras no se asignen, estos están disponibles para tráfico *Best Effort* de la red (que no requiere de solicitud expresa de garantía de recursos).

a) Entidad Funcional de Decisión de Políticas (PD-FE): El Policy Decision Functional Entity representa para la capa de control de servicio un único punto de contacto con la capa de transporte a la hora de autorizar y aplicar reservas de recursos de transporte y QoS. Gracias a este único punto de contacto, se enmascara o esconde la tipología de la red de transporte a un operador de la subcapa de control de servicio.

Las solicitudes de autorización de QoS y reserva de recursos se reciben a través de la capa de control de servicio (a través de una interfaz llamada Rs), desde otro PD-FE perteneciente a otro operador NGN en un escenario de nomacidad o itinerancia (a través de una interfaz llamada Ri), o bien desde otro PD-FE perteneciente al mismo dominio (a través de una interfaz llamada interfaz Rd).

Cuando la petición de recursos de QoS se recibe desde las funciones de la subcapa de control de servicio se dice que la reserva se realiza en modo *push*, porque al final se traduce en un control de admisión y una instalación de políticas de QoS sobre la subcapa de procesado de transporte.

En un modo distinto, el PD-FE también puede recibir dicha solicitud de reserva de recursos desde aquellas entidades funcionales de la subcapa de procesado de transporte que posean la entidad elemental de aplicación de políticas (PE-FE) vía la interfaz Rw.

Cuando la petición de recursos de QoS se recibe desde las funciones de la subcapa de procesado de transporte se dice que la reserva se realiza en modo *pull*. Este modo pretende respetar y aprovechar los mecanismos inherentes de solicitud de recursos (en capa 2) que podrían existir en algunas redes de acceso. Al final se traduce en un control de admisión y una instalación de políticas de QoS sobre la misma subcapa de procesado de transporte.

Nota

Se contempla la posibilidad de que la capa de control de servicio y el RACF (o también dos RACF) puedan ser entidades gestionadas por operadores distintos y de nuevo se incluye dicha función de frontera administrativa y de acceso a través de un único punto de contacto como método de protección.

El resultado de la autorización en la solicitud de recursos, ya sea positiva o negativa, es siempre comunicando a la entidad que ha realizado la solicitud. Además, el PD-FE debe soportar la solicitud de modificación de una petición ya autorizada (lo que conlleva también al correspondiente proceso de autorización) o también la solicitud de terminación de la sesión de reserva de recursos (lo que significa que deberá liberar los recursos asignados así como desinstalar cualquier política de QoS asociada).

Pero ¿qué debe hacer exactamente el PD-FE para tomar la decisión final sobre si autorizar o no una nueva (o modificada) solicitud de recursos en la red de transporte (ya sea de acceso o troncal)?

Para el PD-FE, tomar esta decisión conlleva realizar una lista de control de admisiones a distintos niveles:

- El PD-FE para empezar debe **autorizar la propia solicitud de recursos y QoS en sí**, aplicando:
  - Reglas de políticas de red arbitrarias (por ejemplo, no admitir ninguna solicitud que contenga información de vídeo de ningún operador), que son según el servicio que se solicita y están proporcionadas directamente por los operadores NGN.
  - SLA particulares entre el operador de la red de acceso (almacenados en el RACF) y el operador de la subcapa de control de servicio. Es como

otro tipo de reglas arbitrarias pero aplicadas exclusivamente a un operador de subcapa de control de servicio en particular.

Un SLA (*Service Level Agreement*) se define como un acuerdo de provisión de servicios entre dos entidades (por ejemplo, suscriptor y proveedor de servicio) en el que se comprometen ciertos aspectos de la calidad de los servicios.

- Posteriormente, debe **realizar el control de admisión** a nivel de suscripción de transporte (solo aplicable al caso de red de acceso) para el usuario que solicita el servicio (perfil de QoS proporcionado por el NACF, a través del punto de referencia Ru).

- Finalmente, **consultar** (vía el punto de referencia llamado Rt) **a la entidad funcional que controla los recursos de transporte (TRC-FE) sobre la disponibilidad de los recursos** para dicha solicitud. La respuesta de éste deberá ser tenida en cuenta (el número de TRC-FE conectados al PD-FE dependerá de la tipología de la red de acceso o troncal).

Nota

El PD-FE no realiza el control de los recursos de la red. Para eso está el TRC-FE, al cual le solicita que autorice la reserva de recursos (reserva de capacidad) según la información actualizada del estado de los recursos de la red que éste posee.

Entonces, si la solicitud pasa la autorización y todos estos controles de admisión, ¿qué debe hacer el PD-FE?

Si el resultado de esta autorización de recursos es positivo, el PD-FE puede decidir instalar políticas de QoS (con **parámetros QoS que no dependen de la tecnología** de la red de transporte) sobre los elementos correspondientes para la aplicación de políticas en la subcapa de procesado de transporte (las entidades funcionales que contengan el PE-FE, básicamente). De hecho, puede controlar a varias instancias de PE-FE vía la interfaz Rw siempre y cuando estén dentro del mismo dominio administrativo.

Nota

Estos parámetros de QoS utilizados en las políticas están especificados por la ITU-T en su recomendación Y.1514.

El PD-FE, además, puede interactuar con entidades localizadas dentro de los propios equipos de usuario, y más concretamente, en el caso de que el usuario tenga una pasarela residencial con dispositivos conectados detrás. Estamos hablando de la entidad funcional de aplicación de políticas localizada en la pasarela residencial (CGPE-FE en la figura 4). Se debe tener en cuenta que más allá de la pasarela residencial está el enlace con la red de acceso, así que es muy probable que en esta entidad funcional se produzca un cuello de botella en sentido de enlace de subida y, por lo tanto, debe aplicar algún mecanismo de aplicación de políticas de QoS. Así pues, el PD-FE utiliza el punto de referencia Rh para instalar reglas de políticas directamente en la pasarela residencial y garantizar la QoS según el control de admisión que se realice.

La interfaz Rh'

La interfaz Rh' se usa para el caso de un control más complejo de los recursos en el lado del usuario donde otra entidad llamada CGPD-FE sería capaz de realizar funciones de control de admisión a nivel de recursos, pero en el ámbito de la red local del usuario.

Cuando el PD-FE ha de interactuar con un elemento PE-FE (vía Rw) para instalar una política de QoS, ésta puede incluir información sobre **control de acceso a modo de cortafuegos** (*Gate Control*) si la entidad PE-FE en cuestión lo requiere. Estas reglas de paso son en forma de tupla de 5 parámetros: IP origen y destino, puerto origen y destino y protocolo; o si aplica, identificador de transporte en capa 2 como VLAN ID. Con ellas se permite o deniega el paso de los flujos IP que caracterizan a la sesión del servicio.

Reflexión

Una vez vistas las entidades en la subcapa de procesado de transporte, ¿qué entidades funcionales creéis que pueden ser elegidas por la entidad PD-FE para realizar el control de acceso?

También puede incluir información para que las entidades de la subcapa de procesado de transporte que apliquen puedan realizar el **marcado (o remarcado) de los paquetes IP** si así se requiere, con tal de garantizar cierta QoS a lo largo de la red de acceso o troncal.

Nota

Existen métodos de marcado de paquetes que obedecen a un mecanismo estandarizado de garantía de QoS, como DiffServ. Pero dentro de un dominio, el operador puede adoptar cualquier patrón de marcado (estándar o no) con tal de que se garantice la misma QoS.

Si el elemento de aplicación de políticas PE-FE con el que interactúa es algún tipo de elemento limítrofe con otro dominio administrativo, las políticas de QoS pueden incluir información de **cruce de NAT (traducción de IP privada a IP pública) y/o puertos** para los flujos IP. Esta funcionalidad obliga al PD-FE a interactuar con la capa de control de servicio y el PE-FE de la subcapa de procesado de transporte para realizar las asignaciones de direccionamiento IP y/o puertos en el lado global y local del PE-FE que realiza esta traducción.

Reflexión

¿Tendría sentido una funcionalidad así en una red de transporte que únicamente usara direccionamiento basado en IPv6?

En algunos casos el PD-FE se puede decidir **limitar la velocidad en bits por segundo**[1] de los flujos IP del servicio (por ejemplo, en un servicio de vídeo bajo demanda puede haber un flujo IP para vídeo y otro para audio por separado, que según el codificador que usen no deberían sobrepasar cierta tasa). Pues esta información también se incluye en la especificación de la política QoS a aplicar en las entidades que aplican dichas políticas de QoS en la subcapa de procesado de transporte.

[(1)]Esta función es muy recomendada para tráficos inelásticos, es decir, basados en UDP y más concretamente están recomendados para tráficos multimedia de transmisión de contenidos basados en el protocolo RTP.

Si el PD-FE controla una red troncal, debe poder **controlar el camino que recorren los flujos IP** así como las entradas y salidas de estos flujos en el ámbito que controla. También debe poder localizar las entidades PE-FE dentro de las redes troncales que deben involucrarse en la garantía de QoS extremo a extremo. Todo esto se realiza indicando rutas en la red troncal las cuales están condicionadas por la información recibida desde Rs y las políticas (independientes de la tecnología subyacente).

¿Hace algo más el PD-FE?

Pues el PD-FE puede notificar a las entidades de la subcapa de control de servicio (vía el punto de referencia Rs) sobre eventos ocurridos en la red de transporte si así lo ha requerido la entidad que ha solicitado los recursos de QoS. Estos eventos pueden haber sido reportados por entidades a su cargo (PE-FE vía Rw o TRC-FE vía Rt).

Por ejemplo, reportar la pérdida de conectividad de transporte de cualquier usuario que tenga una sesión de reserva de recursos activa. De esta manera deja a la capa de servicio que ordene al RACF a liberar todos los recursos reservados para tal usuario.

Fijaos en la figura 4 que el PD-FE puede tener interconexión con otras entidades externas, como las de gestión de movilidad (MMFC) vía una interfaz llamada Ro y la de procesamiento de parámetros de gestión (MPM) vía una interfaz llamada Rm. La primera se utiliza para preguntar al RACF sobre la disponibilidad de recursos para un usuario en concreto en la red de acceso antes de realizar el *handover*. La segunda es para reportar información de utilización de la red de acceso o troncal, así como información de monitorización útil.

b) Entidad Funcional de Control de Recursos de Transporte (TRC-FE): El Transport Resource Control Functional Entity realiza decisiones de admisión de solicitudes de recursos remitidas desde el PD-FE a través del punto de referencia Rt. El TRC-FE es una entidad independiente del servicio para la cual se realiza la solicitud de recursos pero a la vez está adaptada a la tecnología específica y a la tipología de la red de transporte cuyos recursos controla.

Sobre la base de esto último, toma una decisión acerca de la admisión o no de los recursos solicitados. Esta decisión se envía en respuesta al PD-FE como uno más de los parámetros que usa éste para tomar la decisión final de control de admisión.

Cabe la posibilidad de que el PD-FE haga dicha solicitud a un solo TRC-FE prefijado y éste distribuya la solicitud debidamente desglosada a otras instancias de TRC-FE (a modo de jerarquía) distribuidas a lo largo de los segmentos que forman la red (todos dentro de un mismo dominio) y con gestión de recursos independiente. Esta comunicación entre TRC-FE se realiza a través de un punto de referencia llamado Rp.

Nota

Tened en cuenta que la comunicación entre TRC-FE adyacentes es siempre intradominio. El estándar de la ITU-T no admite que dos TRC-FE de distinto dominio interactúen. Para ello ya se ha definido la interacción entre entidades PD-FE por el punto de referencia Ri.

Un TRC-FE puede interactuar con más de un PD-FE o con otro TRC-FE adyacente, siempre dentro de su mismo dominio.

El TRC-FE además debe soportar la modificación de la reserva de recursos así como la liberación de los recursos si así lo indica el PD-FE.

Pero ¿cómo toma el TRC-FE la decisión sobre la disponibilidad o no de los recursos solicitados?

El TRC-FE es el elemento que realmente se adapta a la tecnología concreta de la red de acceso o troncal, conociendo exactamente los mecanismos y los parámetros de QoS relacionados con la tecnología en cada segmento. Y para poder realizar un control exhaustivo de los recursos, se vale de una interfaz llamada Rc para solicitar y captar todo tipo de información que le ayude a tener actualizada la tipología y estado de los recursos. Esta interfaz Rc, la cual es totalmente dependiente de la tecnología subyacente de la red de transporte, conecta al TRC-FE con todas aquellas entidades de la subcapa de procesado de transporte que le puedan proporcionar dicha información (no se cierra la puerta a que el TRC-FE sea completamente autónomo sin necesitar de dicha interfaz Rc).

Además, sobre la base del resultado de ese control de admisión, es capaz de actualizar y asignar los recursos en el segmento agregado de la red para cumplir con la QoS solicitada desde el PD-FE. Para ello, utiliza la interfaz Rn, que le comunica con la entidad que asigna los recursos en la subcapa de procesado de transporte (TRE-FE).

¿Cómo solicita los recursos el PD-FE al TRC-FE?

Dependerá de si la reserva de recursos de QoS en el PD-FE se realiza en modo *push* o modo *pull*. Si es en modo *push*, el PD-FE puede recibir la solicitud de nueva reserva de recursos de QoS en dos fases (reserva en la primera fase y asignación en la segunda) o en una sola (reserva + asignación en una sola). El procedimiento de reserva (*Reserve*) y asignación (*Commit*) de recursos en dos fases responde al propio PD-FE, que lo especifica así porque también así se lo han especificado vía Rs.

Digamos que si el PD-FE, una vez ha autorizado la petición de QoS, le indica que quiere solo "reservar" los recursos, el TRC-FE realiza el control de admisión de capacidad global del sistema, actualiza el estado de dichos recursos y le da respuesta al PD-FE, pero no ejecuta la asignación de recursos ni una instalación de políticas de QoS sobre el TRE-FE (ni tampoco lo hará el PD-FE sobre el/los PE-FE). Es cuando el PD-FE recibe una modificación de la sesión de solicitud de recursos donde se indica que en ese momento se quiere hacer uso de los recursos reservados y solicita la asignación.

3) Control de Gestión de la Movilidad (MMCF)

La ITU-T ha definido este conjunto de funciones claramente para copar con aquellas redes cuyos equipos de usuario ya no están basados en una pasarela residencial, sino que son un solo dispositivo y que además tienen la capacidad de la movilidad: las redes móviles (LTE), Wi-Fi o WiMAX.

Nota

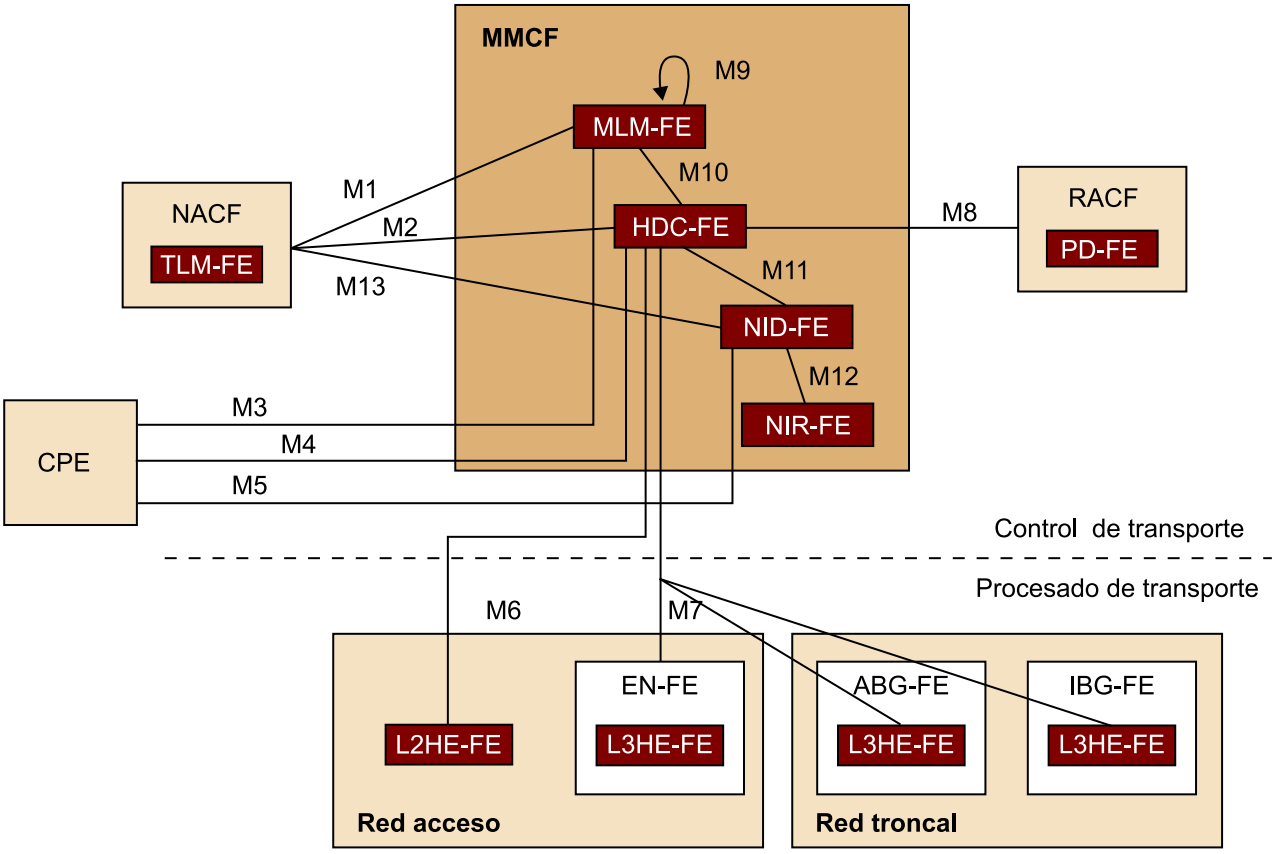
El terminal de usuario puede soportar más de una tecnología inalámbrica simultánea (los *smartphones* soportan LTE y Wi-Fi) con lo que se convierten en lo que podemos llamar un terminal híbrido.

Y es en estos casos donde la capacidad de movilidad cobra una gran importancia a nivel de control de transporte. Las redes fijas (ADSL, cable, fibra, etc.) no tendrían necesidad de tener que soportar o implementar estos bloques de movilidad.

El MMCF se encarga básicamente de posibilitar a un usuario que posee un terminal móvil realizar un *handover* a nivel de red de transporte de manera transparente para el usuario copando incluso el mecanismo a nivel de subcapa de control de transporte para la transferencia de sesiones de reservas de recursos que ese terminal pudiera tener activas.

Dependiendo de la tecnología de la red este proceso de *handover* puede ser liderado por el propio terminal de usuario (con apoyo de la red) o por la red.

Figura 5. Arquitectura de referencia del MMCF



Dentro de la movilidad se pueden describir dos modos de operación:

- **Movilidad controlada por el equipo de usuario**: Es un modo de operación donde el equipo de usuario toma un papel activo en la provisión del servicio de movilidad en capa 3, concretamente contactando con el proveedor de servicio de movilidad para invocar este servicio tan pronto como consigue el ingreso en la red.

- **Movilidad controlada por la red**: Es el modo de operación donde el equipo de usuario no toma un papel activo en la provision del servicio de movilidad. Toda la iniciativa la lleva la red.

A continuación vamos a ver una descripción entidad a entidad del MMFC y la relación entre cada una de ellas.

Ved también

Un resumen de los puntos de referencia involucrados con este bloque funcional se puede encontrar en la tabla 6 del anexo.

a) Entidad Funcional de Gestión de Localización Móvil (MLM-FE). El Mobile Location Management Functional Entity tiene una serie de responsabilidades relacionadas con la movilidad, las cuales se resumen en la siguiente lista:

- Si la movilidad está controlada y liderada íntegramente por la red, el MLM-FE se encargaría de registrar la localización inicial en el nombre del equipo de usuario.

- Procesa mensajes de registro de localización enviados desde (vía M3) o en el nombre del equipo de usuario (vía M1).

- Opcionalmente, mantiene la asociación entre el identificador de usuario en el servicio de movilidad y la dirección IP asignada de manera persistente al usuario.

- Gestiona la asociación entre la dirección IP persistente asignada a un equipo de usuario y la dirección temporal, si se trata de movilidad controlada y liderada por el *host*, o la dirección del extremo del túnel más cercano al equipo de usuario, si se trata de movilidad basada en red (esta tecnología basada en túneles o *bearers* es muy utilizada en tecnología LTE y WiMAX).

- De manera opcional, mantiene dos asociaciones de localización para el equipo de usuario móvil marcando la asociación para la red presente como "activa" y marcando la asociación para la red objetivo como "standby".

- Soporta la separación del plano de control y de datos permitiendo que la dirección del MLM-FE y la dirección del terminal para el traspaso de datos (la dirección del túnel del terminal) sean diferentes.

- Indica una nueva asociación de movilidad y distribuye la información de la asociación al HDC-FE (vía M10).

b) Entidad Funcional de Control y Decisión de Handover (HDC-FE). El Handover Decision and Control Functional Entity tiene tres subfunciones:

- Decisión de *handover* (HDF): recibe desde el equipo de usuario una lista de enlaces de acceso de candidatos para realizar un *handover* e invoca al o los RACF para verificar la disponibilidad de los recursos de QoS para cada uno de los enlaces. También solicita al RACF reasignación de recursos y QoS en el nuevo camino de datos (libera los recursos del antiguo camino

a la vez que configura los recursos en el nuevo). Además, puede disparar el *handover* bajo la petición del equipo de usuario (en el caso de liderazgo de la movilidad desde la red). En ese caso puede comunicar la acción de *handover* al elemento de ejecución en capa 2 L2HCF (si el *handover* es dentro de la subred) y al L3HCF (si el *handover* es entre subredes).

- Control de *handover* en capa 2 (L2HCF): se comunica con la entidad L2HE-FE en la subcapa de procesado de transporte para transferir eventos de la capa de enlace hacia el HDF y, bajo petición de éste, invocar el *handover* a la instancia apropiada del L2HE-FE.

- Control de *handover* en capa 3 (L3HCF): se comunica con la entidad L3HE-FE en la subcapa de procesado de transporte para, bajo petición de éste, invocar y coordinar el *handover* a las instancias apropiadas del L3HE-FE.

c) Entidad Funcional de Distribución de Información de Red (NID-FE). El Network Information Distribution Functional Entity se responsabiliza de lo siguiente:

- Distribuye las políticas de *handover*, que son un grupo de reglas y preferencias definidas por los operadores NGN que afectan a las decisiones tomadas por el equipo de usuario o el HDC-FE. Se distribuyen al equipo de usuario vía la interfaz M4 y al HDC-FE vía la interfaz M11.

  Por ejemplo, una política de *handover* puede indicar que un *handover* vertical desde una red de acceso E-UTRAN (LTE) a una red de acceso Wi-Fi no está permitido. Podría indicar además que la red de acceso WiMAX es preferible a Wi-Fi.

- Distribuye otra información proporcionada por el NIR-FE (recibida desde la interfaz M12).

d) Entidad Funcional de Repositorio de Información de Red (NIR-FE): El Network Information Repository Functional Entity proporciona información estática sobre redes vecinas al NID-FE para darle apoyo en el descubrimiento de las redes de acceso y en la toma de decisión de la selección de la siguiente red.

1.2.2. Arquitectura de referencia del ETSI TISPAN

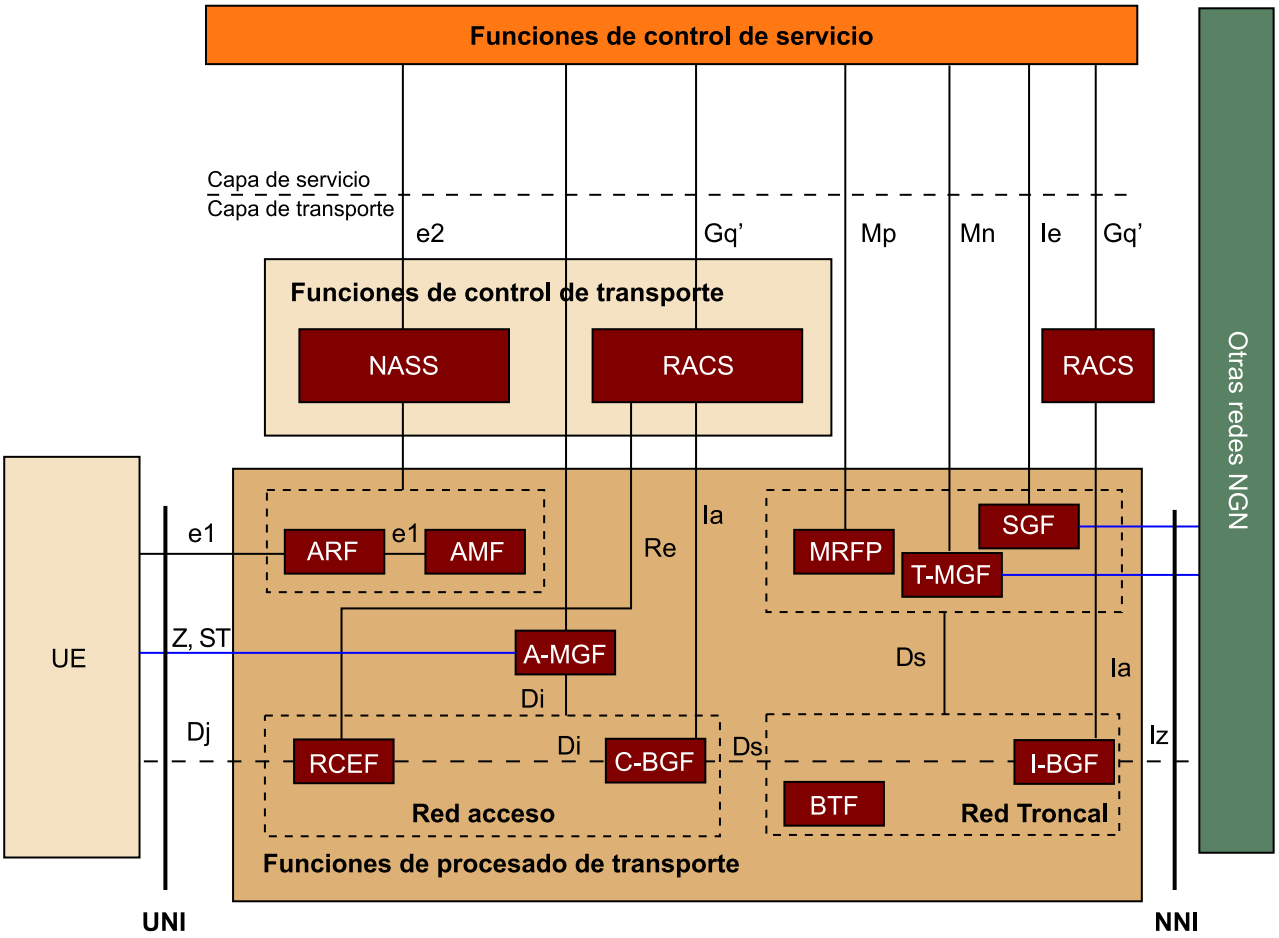
La ETSI-TISPAN también define la capa de transporte de las redes NGN. La descripción de algunos bloques es calcada a los descritos en la ITU-T, solo que cambiando nombres de las entidades funcionales y las interfaces. En otras ocasiones sí que se produce alguna variación con respecto a la ITU-T.

Veremos que la ETSI-TISPAN ha elegido el camino de la integración en redes NGN de las redes de acceso fijas. Lo notaréis en el tipo de equipo de usuario que contempla y en que hay funcionalidades que no especifica, como la gestión de la movilidad.

Subcapa de procesado de transporte

En este apartado veremos una descripción funcional de las entidades que conforman la subcapa de procesado de transporte según el modelo de la ETSI-TISPAN, subdividas en red de acceso y red troncal. La arquitectura de referencia de la ETSI-TISPAN se muestra en la figura 6.

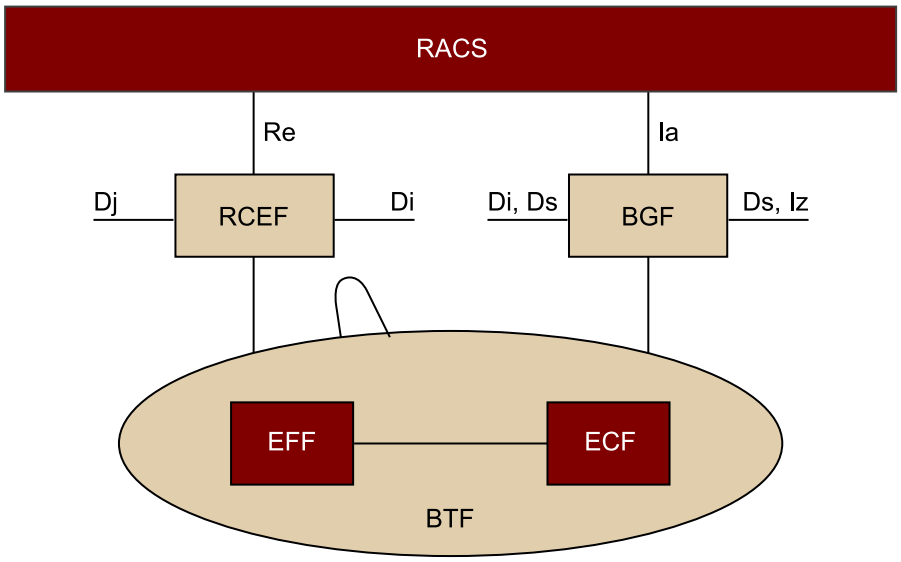
Figura 6. Arquitectura de referencia de la subcapa de procesado de transporte para la ETSI-TISPAN



1) Funcionalidad Básica de Transporte (BTF)

Como en el modelo de referencia de la ITU-T, la ETSI-TISPAN también define entidades funcionales elementales que afectan a la simple transferencia de paquetes IP. En este caso se trata del Basic Transport Function (BTF), la cual se subdivide en dos elementos más sencillos: la entidad elemental de transferencia de paquetes (EFF) y la de control (ECF).

Figura 7. Componentes del BTF



Como podemos ver en la figura 7, el BTF tiene la capacidad de interactuar con dos elementos que procesan el tráfico de usuario:

- el RCEF, que es la entidad que aplica políticas de QoS dictadas desde el bloque que controla los recursos de la red de transporte (RACS) y
- la entidad fronteriza con otras redes de transporte de diferente dominio administrativo (BGF).

Un ejemplo de esta interactuación entre BTF y el RCEF o el BGF es el modo *pull*, donde se les notifica sobre eventos relacionados con la tecnología de la red de transporte y que pueden desencadenar una reserva de recursos. La interfaz entre el RCEF o el BGF y este elemento está fuera del ámbito de la especificación, ya que depende mucho de la tecnología de la red.

Veamos la descripción de estas dos entidades elementales según la ETSI-TIS-PAN:

- **Funcionalidad Elemental de Transferencia (EFF):** Corresponde exactamente en funciones con la entidad elemental definida por la ITU-T, EF-FE descrita anteriormente.

- **Funcionalidad Elemental de Control (ECF):** Corresponde exactamente en funciones con la entidad elemental definida por la ITU-T, EC-FE descrita anteriormente.

2) Entidades funcionales de procesado de transporte en la red de acceso

Continuando la misma clasificación de entidades funcionales de la subcapa de procesado de transporte seguida en la especificación de la ITU-T, vamos a explicar qué entidades corresponderían a la red de acceso y qué paralelismos tienen con las entidades equivalentes de la ITU-T. Si miramos a la arquitectura de referencia de la figura 6, podemos ver un total de 4 entidades funcionales.

a) Funcionalidad de Pasarela de Medios de Acceso (A-MGF): El Access Media Gateway Function interconecta la red de acceso NGN con terminales de usuario con tecnología de redes tradicionales de telefonía (RTC y RDSI). Así pues, equivale a la entidad funcional AMG-FE de la ITU-T[2].

b) Funcionalidad de Aplicación de Control de Recursos (RCEF): El Resource Control Enforcement Function es una entidad funcional que se encarga primordialmente de aplicar las políticas de QoS que el RACS le indica, vía un punto de referencia llamado Re. Estas políticas, llamadas *Policy Rules*, pueden estar predefinidas en el propio bloque y el RACS simplemente ha de hacer referencia a ellas para activarlas o desactivarlas. O bien el RACS las puede definir por completo indicando parámetros de clasificación de tráfico (flujos IP), nivel de prioridad (marcado de ToS) e identificadores de clasificación de transporte.

El RCEF puede actuar en modo *push* en la asignación de recursos, donde recibe estas políticas desde el RACS y las aplica **mapeando los parámetros de QoS de la política** (independientes de la tecnología subyacente) con parámetros específicos de la tecnología de la red de acceso.

El RCEF puede actuar también en modo *pull*, en el que recibe una notificación desde la entidad elemental BTF (dependiente de la tecnología de la red de acceso) diciendo que un equipo de usuario solicita recursos. El RCEF reformatea el mensaje acorde a la especificación de la interfaz Re para notificárselo al RACS y esperar una toma de decisión por parte de éste (en forma de instalación de nuevas políticas).

Independientemente al modo en el que trabajemos, el RCEF puede **reportar eventos** a nivel de capa de transporte que puedan provocar una toma de decisión del RACS acerca de las políticas de QoS activas (las puede eliminar o modificar, dependiendo de las políticas del operador).

Trazando un paralelismo con el modelo de referencia de la ITU-T, el RCEF se corresponde con las entidades funcionales equivalentes de la ITU-T en procesado de transporte como el AN-FE o CGPE-FE, éste en el lado del equipo de usuario. Es decir, se ubica en aquel lugar donde hay potencialidad de cuello de botella o donde se tiene que realizar asignación directa de recursos en la red de acceso.

c) Funcionalidad de Pasarela Fronteriza (C-BGF): Sobre el Core Border Gateway Function, como se llama en inglés, se puede decir que equivale a la entidad funcional de la ITU-T llamada *EN-FE*, entidad funcional fronteriza entre la red de acceso y la red troncal de distinto dominio administrativo, exceptuando las funciones que afectan a la movilidad en capa 3, las cuales no son implementadas en el modelo de la ETSI-TISPAN. El C-BGF es controlado por

(2)Ver el subapartado "Subcapa de control de transporte".

Nota

La ETSI también define un subtipo del A-MGF: el R-MGF (*Residential*), que viene a ser lo mismo que el A-MGF, pero integrado en la pasarela residencial (localizadas en instalaciones del usuario).

Clasificadores de transporte

Los llamados clasificadores de transporte, que la ETSI-TISPAN indica, son muy útiles para relacionar las políticas de QoS a aplicar a la conectividad con el equipo de usuario en cuestión, por ejemplo, un identificador de canal virtual en ATM.

el bloque de Control Admisión y Recursos (RACS) en la subcapa de control de transporte a través de un punto de referencia llamado Ia, que equivale en funciones a la interfaz Rw de la ITU-T.

d) Funcionalidad de Retransmisión de Red de Acceso (ARF): El Access Relay Function equivale exactamente a la entidad funcional del modelo de la ITU-T llamado *AR-FE*. Se interconecta con el NASS, el bloque de funciones equivalente al NACF de la ITU-T para la adhesión a la red de acceso.

3) Entidades funcionales de procesado de transporte en la red troncal

Pasamos la frontera de la red de acceso para pasarnos al ámbito de la red troncal de alta capacidad. En este ámbito identificamos un total de cuatro entidades. Veremos cómo hay un paralelismo muy claro con las entidades de procesado de transporte de la red troncal en el modelo de referencia de la ITU-T.

a) Funcionalidad de Pasarela Fronteriza (I-BGF): Sobre el Interconnection Border Gateway Function, como se llama en inglés, se puede decir que equivale a la entidad funcional de la ITU-T llamada IBG-FE, entidad funcional fronteriza entre dos redes troncales de distinto dominio administrativo, exceptuando las funciones que afectan a la movilidad en capa 3, las cuales no son implementadas en el modelo de la ETSI-TISPAN. El I-BGF es controlado por el bloque de Control Admisión y Recursos (RACS) en la subcapa de control de transporte a través de un punto de referencia llamado Ia, que equivale en funciones a la interfaz Rw de la ITU-T.

b) Funcionalidad de Pasarela hacia Redes de Circuitos (T-MGF): equivale a la entidad funcional TMG-FE de la ITU-T. La interfaz que le conecta con el elemento de la capa de control de servicio es la llamada Mn (equivalente a la interfaz S-T4 definido por la ITU-T).

c) Procesado de Funcionalidades de Recursos Multimedia (MRFP): El Multimedia Resource Function Processor equivale exactamente a la entidad funcional MRP-FE del modelo de la ITU-T. La interfaz que le conecta con el elemento de la capa de control de servicio es la llamada Mp (equivalente a la interfaz S-T1 definida por la ITU-T).

d) Funcionalidad de Pasarela de Señalización (SGF): La Signalling Gateway Function equivale exactamente a la entidad funcional SG-FE del modelo de la ITU-T. La interfaz que le conecta con el elemento de la capa de control de servicio es la llamada Ie (equivalente a la interfaz S-T3 definida por la ITU-T).

Subcapa de control de transporte

Del mismo modo que en el modelo de la ITU-T, en la subcapa de control de transporte radica la inteligencia de gestión de recursos tanto de la red de acceso como de la red troncal. Define los mismos puntos de referencia abiertos que les

conectan con la capa de servicio y que proporcionan la independencia entre la tecnología de la red de transporte y los servicios con garantía de QoS extremo a extremo. Esta subcapa está formada por dos bloques principales: el de Control de Adhesión a la Red (NASS en sus siglas en inglés), el de Control de Admisión y Recursos (RACS). A diferencia del modelo de la ITU-T, el de la ETSI-TISPAN no contempla ningún bloque de funciones que gestione la movilidad, ya que se centra en la integración de redes fijas en las redes NGN.

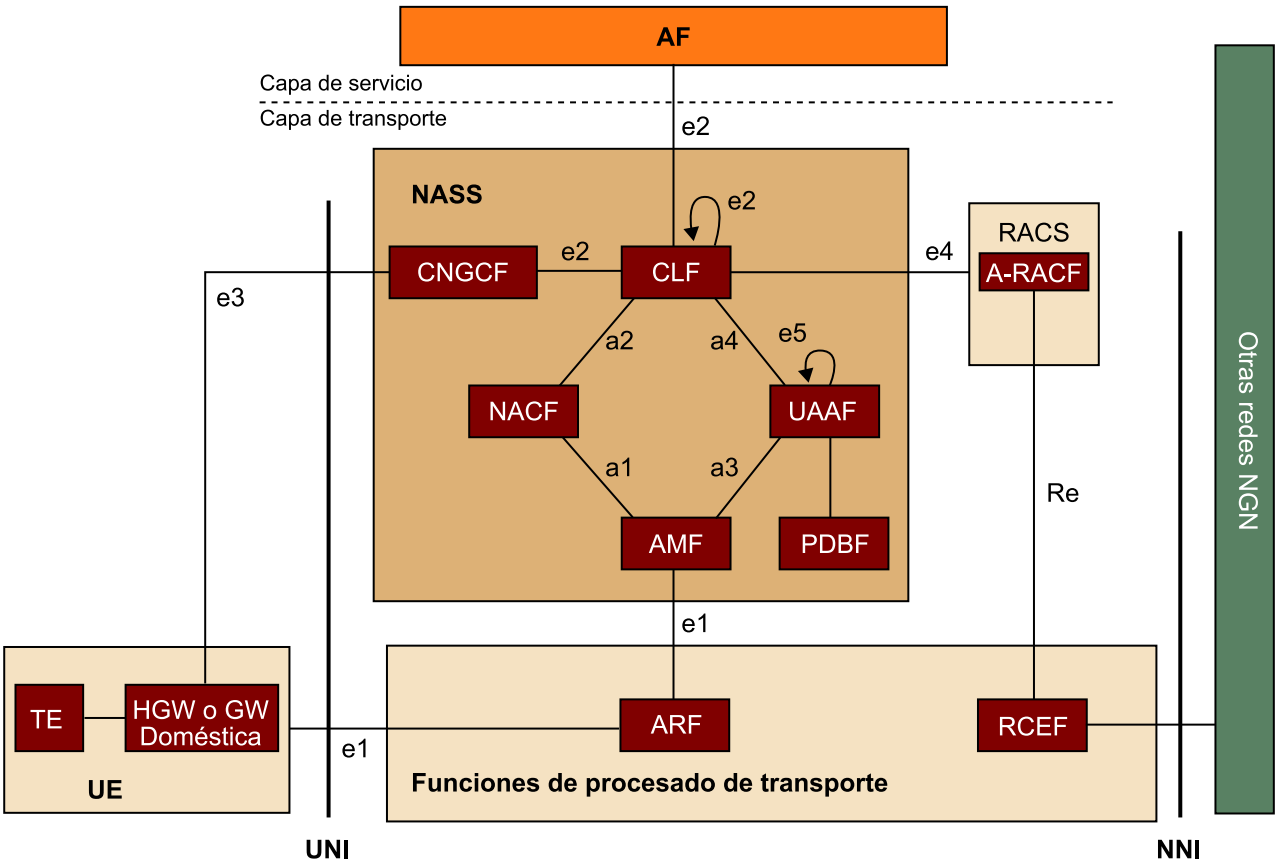
1) Subsistema de Adhesión a la Red (NASS)

El siguiente diagrama muestra la composición de la arquitectura de referencia para el NASS según la ETSI-TISPAN. Equivale íntegramente entidad tras entidad e interfaz tras interfaz al modelo de la ITU-T, el NACF, con excepción de la ausencia de interactividad con algún bloque que gestione la movilidad en la capa de transporte.

Ved también

En la tabla 7 del anexo se puede ver un resumen de los puntos de referencia del NASS.

Figura 8. Arquitectura de referencia del NASS para la ETSI-TISPAN



Nota

La ETSI-TISPAN se ha especializado en integrar las redes fijas cableadas en el estándar de las redes NGN y es por ello por lo que el estándar de la ETSI para NGN no contempla interfaces (puntos de referencia) a ningún bloque funcional que gestione la movilidad en la capa de transporte. Los terminales son fijos y por lo tanto, no hay movilidad que soportar, al menos tal y como la entendemos en las redes móviles de 3GPP.

a) Funcionalidad de Configuración de Acceso a la Red (NACF): El Network Access Configuration Function equivale exactamente con la entidad funcional NAC-FE del modelo de la ITU-T para el NACF, con la única salvedad de que asigna una IP y no dos (solo la IP persistente al no haber movilidad). Del mismo modo los puntos de referencia llamados a1 y a3 corresponden al Nd y Na del modelo de la ITU-T respectivamente.

b) Funcionalidad de Autenticación y Autorización del Usuario (UAAF): El User Authentication and Authorizaction Function (UAAF) equivale exactamente a la entidad funcional TAA-FE del modelo de la ITU-T para el NACF (inclusive sus funcionalidad de proxy en un escenario de itinerancia). Del mismo modo que los puntos de referencia llamados a3, a4 y e5 corresponden al Na, Nc y Ni del modelo de la ITU-T respectivamente.

Nota

Así como en el modelo de la ITU-T se define un punto de referencia entre el TAA-FE y el TUP-FE, en la ETSI-TISPAN no especifican ninguno (libertad total de especificación) entre el UAAF y el PDBF.

c) Funcionalidad de Base de Datos de Perfiles (PDBF): El Profile Data Base Function (PDBF) es, como su nombre indica, el lugar donde se almacena toda la información de credenciales y perfiles de QoS a nivel de transporte. En definitiva, equivale exactamente al TUP-FE de la ITU-T. El formato de los perfiles de usuario es equivalente a los de la ITU-T.

Lectura complementaria

Más información sobre el formato propuesto para dichos perfiles la podéis encontrar en el documento ES 282 004.

d) Funcionalidad de Repositorio y Localización de Conectividad de Sesión (CLF): El Connectivity session Location and repository Function equivale exactamente a la entidad funcional TLM-FE del modelo del modelo de la ITU-T para el NACF (inclusive su funcionalidad de proxy en un escenario de intinerancia con un CLF de otro dominio). Del mismo modo que los puntos de referencia llamados a2, a4, e2 y e4 corresponden al Ne, Nc (S-TC1, Ng y Nx) y Ru del modelo de la ITU-T respectivamente.

Vemos que la interconexión con la subcapa de control de servicio (para la ETSI se llama Application Function o AF) se realiza a través del punto de referencia e2, pero a diferencia del ITU-T, se especifica la misma interfaz para interconectar el CLF con el CNGCF (el equivalente de HGWCFE con su interfaz Nx) y que el que interconecta el CLF visitado con el CLF local (modo itinerancia a nivel de CLF).

Para el ETSI-TISPAN, se define el AF como aquella entidad de la capa 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 RACS vía la interfaz Gq'. Si el servicio está basado en IMS, el AF será el P-CSCF y si no está basado en IMS, será una entidad equivalente.

e) Funcionalidad de Configuración de la Pasarela de la Red del Cliente (CNGCF): El Customer Network Gateway Configuration Function (CNGCF) equivale exactamente a la entidad funcional HGWC-FE del modelo de la ITU-T para el NACF. Del mismo modo que los puntos de referencia e2 y e3 corresponden al Nx y TC-Ux del modelo de la ITU-T respectivamente.

Pasarela residencial (CNG)

La ETSI-TISPAN considera, casi como la única opción, que el equipo de usuario o UE esté formado por una pasarela residencial (CNG) y detrás toda una red local de cliente con dispositivos conectados. En esta pasarela CNG, como en el elemento equivalente de la ITU-T para pasarelas residenciales, se desarrollan las funciones de usuario, como por ejemplo:

- aplicación de políticas de QoS desde el RACS;
- interfaz para autenticación de los usuarios en la red local (en apoyo del NASS);
- traducción de protocolos de señalización a IMS para soportar terminales de otras tecnologías en dicha red local;
- aplicación de traducciones de direcciones IP o puertos (NAT o NAPT).

La ETSI-TISPAN ha dedicado esfuerzos en la definición concisa de las funciones de usuario atribuidas a una CNG. Una descripción más detallada (con bloques funcionales y todos los puntos de referencia) las podéis encontrar en el documento TS 185 003.

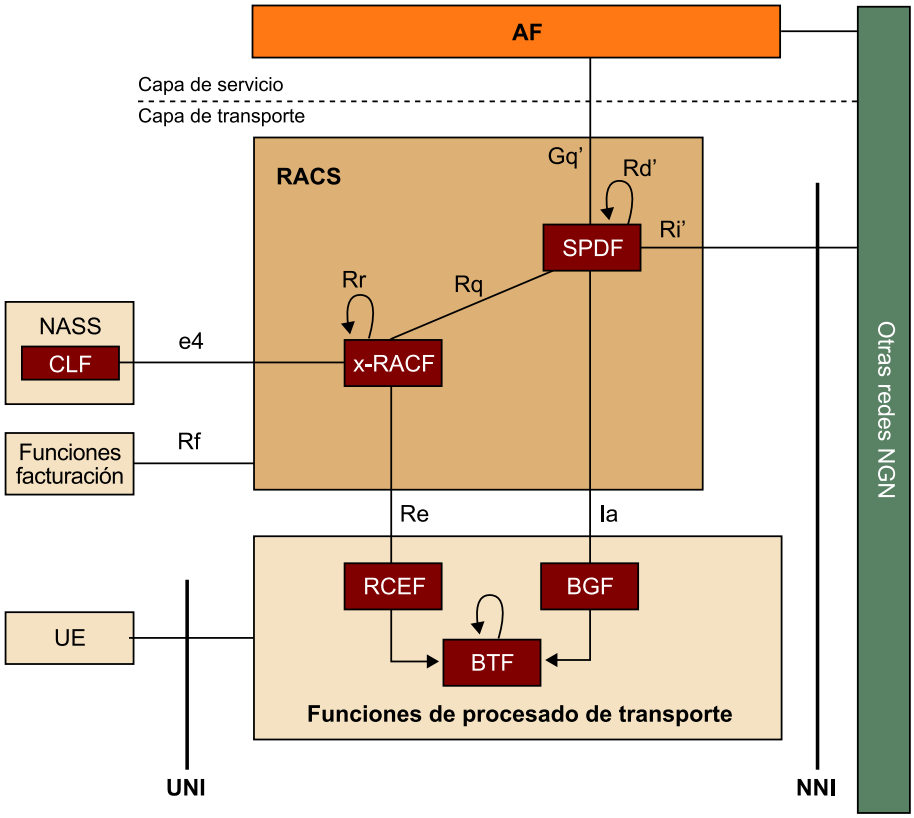
2) Subsistema de Control de Admisión y Recursos (RACS)

La figura 9 muestra la arquitectura funcional de referencia del RACS. Aunque mantiene muchas similitudes con la arquitectura de referencia de la ITU-T del RACF, sí que guarda ciertas diferencias a nivel de distribución de funciones de control de admisión entre los bloques que la forman. El RACS está formado por 2 entidades funcionales, las cuales vamos a describir a continuación.

Ved también

En la tabla 8 del anexo podéis encontrar un resumen de las interfaces del RACS.

Figura 9. Arquitectura de referencia del RACS para ETSI-TISPAN



a) Funcionalidad de Decisión de Políticas de Servicio (SPDF): El Service Policy Decision Function, como su equivalente en el modelo de la ITU-T (PD-FE), representa para la subcapa de control de servicio (AF) un único punto de contacto con la capa de transporte a la hora de autorizar y aplicar reservas de recursos de transporte y QoS.

El SPDF aplica lo que se conoce como **políticas basadas en servicios** para tomar la decisión final sobre la aceptación o no de la solicitud de nueva sesión de reserva de recursos de QoS, así como la modificación de una sesión ya activa. A esta reserva la ETSI-TISPAN la llama sesión de servicio de control de transporte. Dichas solicitudes pueden ser recibidas desde el AF (modo *push*) vía un punto de referencia llamado *Gq'* o desde otro SPDF adyacente vía una interfaz llamada Ri ' (si es de otro dominio administrativo a modo de itinerancia) o vía una interfaz llamada Rd' (si son del mismo dominio). El resultado de dicha decisión, ya sea positiva o negativa, debe notificarse al AF o SPDF adyacente vía la interfaz desde donde se haya recibido la petición.

Una **política basada en servicio** es aquella política diseñada para ser aplicada por el SPDF. Está formada por una condición acerca del servicio descrito en la petición recibida y por una acción a tomar si la condición se cumple. La condición está basada en la comparación de parámetros incluidos en la información recibida en la petición con valores especificados en la propia política. Si la comparación cumple con la política, entonces la solicitud es autorizada y se procede a la acción, la cual puede pasar por interrogar a otros elementos del RACS o de la subcapa de procesado de transporte sobre los recursos disponibles (el x-RACF, el BGF, otro SPDF o cualquier combinación de ellos).

El SPDF debe soportar la solicitud de terminación de la sesión de reserva de recursos. Ello desencadena en el x-RACF la liberación de recursos y la desinstalación de las políticas que se les apliquen.

Un SPDF puede comunicarse con más de un AF y con otros SPDF adyacentes (ya sea dentro de su dominio administrativo o en uno diferente a modo de itinerancia).

Para la ETSI-TISPAN ¿qué pasos tiene que dar el SPDF para tomar la decisión final sobre si autorizar o no una nueva (o modificada) solicitud de recursos en modo *push* en la red de transporte (ya sea de acceso o troncal)?

Para el SPDF tomar esta decisión conlleva realizar una lista de control de admisiones similar a las llevadas a cabo por el PD-FE de la ITU-T, así como esperar la notificación de otros elementos del RACS:

- Debe **autorizar la propia solicitud de recursos de QoS** aplicando reglas de políticas de red arbitrarias a nivel de servicio, así como SLA particulares con el operador del AF.

- Debe **solicitar la reserva y/o asignación de los recursos en la red de transporte** siempre y cuando la solicitud recibida haya sido autorizada. En tal caso, la propia política de servicio le dirá al SPDF que otros elementos del RACS deberán consultar (a uno o más x-RACF) para la reserva de recursos y/o a un C/I-BGF para la traducción de puertos o habilitación de acceso de cortafuegos. La respuesta de esa consulta o consultas condicionará la decisión final a tomar.

El **SPDF no tiene conocimiento en absoluto acerca de la topología ni de la tecnología** subyacente de la red de acceso (o troncal, si fuera el caso). Tampoco tiene acceso a información de perfil de subscripción de usuario ni del estado de los recursos del sistema. Ese es uno de los servicios que solicita al x-RACF vía una interfaz llamada Rq (esta interfaz es intradominio), cuya respuesta es necesaria para poder tomar la decisión final. En el caso de que existiese un C/I-BGF en la red de transporte, el SPDF solicitaría a éste el servicio de asignación de traducción de **dirección de IPs y/o puertos**, **control de limitación de velocidad**, **habilitación de acceso** (*Gate Control*) y **marcado de paquetes**. La respuesta a esta solicitud enviada desde el C/I-BGF (vía la interfaz Ia) debería tenerse en cuenta también antes de enviar la respuesta al AF.

¿Hace algo más el SPDF?

Pues el SPDF puede notificar al AF (vía el punto de referencia Gq') sobre eventos ocurridos en la red de transporte si así lo ha requerido la entidad que ha solicitado los recursos de QoS. Estos eventos pueden haber sido reportados por entidades a su cargo (C/I-BGF vía Ia o x-RACF vía Rq).

Aparte de todo esto, el SPDF es capaz de **procesar la prioridad de petición de servicio**. Es decir, el AF o SPDF interconectado puede indicar al SPDF en la solicitud un nivel de prioridad de servicio (servicio de control de transporte). De acuerdo a ese nivel, el SPDF puede definir un nivel de prioridad de servicio en su solicitud de reserva de recursos enviada al x-RACF.

b) Funcionalidad Genérica de Control de Admisión de Recursos (x-RACF): El Resource and Admission Control Function es una entidad funcional que recibe solicitudes de servicio de reserva y/o asignación de recursos desde el SPDF a través de la interfaz Rq (si la reserva es en modo *push*) o desde el RCEF vía la interfaz Re (si la reserva es en modo *pull*).

x-RACF y SPDF

El x-RACF y el SPDF con el que está interconectado siempre estarán en el mismo dominio. No se contempla ningún punto de referencia de interconexión entre dos x-RACF que pertenezcan a distintos dominios administrativos (la itinerancia a nivel de solicitud de recursos es siempre a nivel de SPDF).

El x-RACF realmente es un punto de decisión más donde se realiza un nuevo control de admisión distinto al que hace el SPDF (aplicable tanto a tráfico *unicast* como *multicast*). El resultado de dicha decisión deberá notificarse al SPDF tras la recepción de la petición.

No obstante, los tipos de control que realiza dependen del tipo de x-RACF que se implemente. La ETSI-TISPAN contempla dos tipos:

- **A-RACF (*Access*)**: Se trata del que está situado en el ámbito de la red de acceso. Con lo cual realiza doble control de admisión: primero comprueba que la petición de recursos entra **dentro del perfil QoS de suscriptor** del usuario que los solicita y segundo, **comprueba que hay suficientes recursos** en la red de acceso para reservar y/o asignar dichos recursos. Para

realizar el control de perfil de suscriptor puede acceder a la información de perfil a través de una interfaz llamada e4, que le conecta con la entidad funcional de Repositorio y Localización de Conectividad de Sesión (CLF) dentro del bloque de Control de Adhesión a la Red (NASS).

Control de suscripción de usuario

La función de control de suscripción de usuario solo se aplica al A-RACF y debe autenticar y autorizar los recursos que solicitan las entidades funcionales (RCEF en modo *pull* y SPDF u otro RACF en modo *push*) en nombre de un suscriptor. Debe comprobar que la solicitud de recursos esté dentro de los parámetros esperados según el perfil del suscriptor, o dicho de otro modo, que un suscriptor no solicite más recursos de los que ha contratado.

- **C-ARACF (*Core*)**: En este caso se trata del que está situado en el ámbito de la red troncal. Con lo cual solo realiza la **comprobación de que hay suficientes recursos**. Esta implementación no realiza el control de admisión sobre el perfil QoS del suscriptor (con lo cual no tiene interfaz e4).

En ambos casos, si al final el control de admisión ha sido satisfactorio y la solicitud de recursos recibida así lo especifica, el x-RACF asigna los recursos solicitados y puede decidir si es necesario instalar y aplicar políticas de QoS sobre las entidades de aplicación de políticas de QoS de la subcapa de Procesado de Transporte (RCEF) vía la interfaz Re.

Nota

Al igual que con el caso del TRC-FE de la ITU-T, el x-RACF y el SPDF deben soportar la reserva de recursos en dos fases (*Reserve* y *Commit*) o en una sola fase (*Commit*) para el caso de reserva en modo *push*.

El x-RACF es un elemento que conoce la topología de la red de acceso o troncal pero las políticas de QoS que confecciona contienen mayoritariamente parámetros de QoS independientes de la tecnología de la red de acceso. Será el RCEF quien, al instalarlas, traducirá estos en unos parámetros equivalentes adaptados a la tecnología de la red de acceso.

Nota

Cada política de QoS lleva asociado un nombre que la identifica de manera única con respecto a otras políticas. Y su estado de activación o desactivación en el RCEF va íntimamente ligado al estado de la sesión de petición de recursos que las ha creado. Con lo cual cuando se recibe una solicitud de terminación de dicha sesión de reserva desde el SPDF (*modo push*) o RCEF (*modo pull*) las correspondientes políticas deben ser desinstaladas.

Según la complejidad de la red de transporte (con varios segmentos susceptibles de una gestión particular de algunos recursos) el x-RACF se puede multiplicar en varias instancias dentro del mismo dominio repartidas por varias partes de la red. Así pues, un x-RACF puede recibir una solicitud de recursos desde el SPDF y a continuación puede delegar el control de parte o todos los recursos en otras instancias de RACF. El intercambio de información entre x-RACF se realiza vía un punto de referencia intra-dominio llamado Rr.

Aparte de todo esto, el x-RACF es capaz de **procesar por separado la prioridad de petición de medios por un lado y de servicio por otro**. También es capaz de procesar eventos recibidos desde el RCEF sobre la red de transporte y reenviarlos al SPDF.

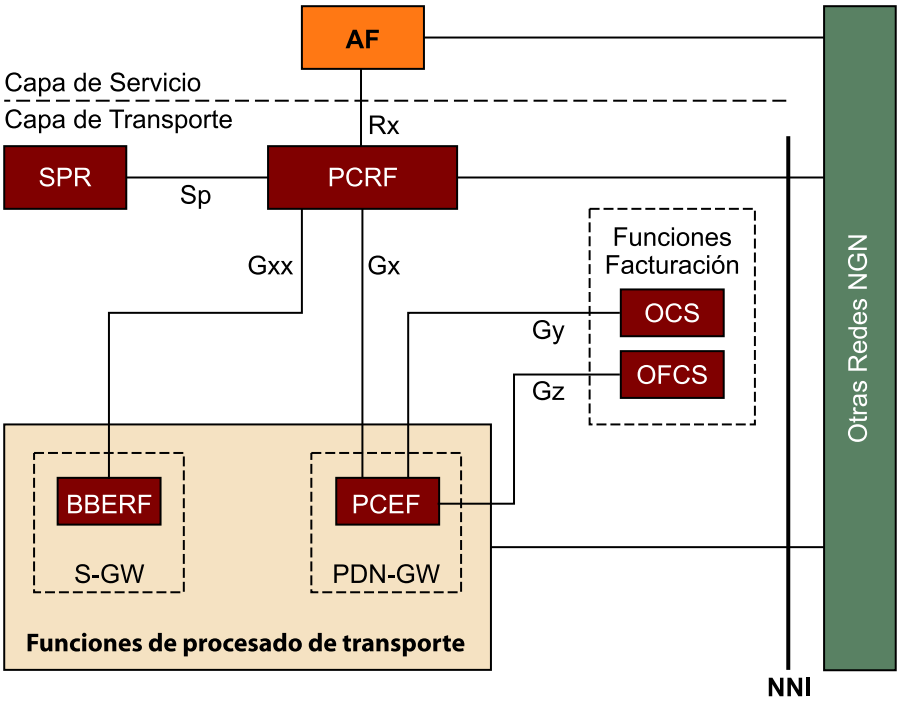
¿Qué significa el nivel de prioridad de medios?

El estándar define que para la solicitud de recursos el SPDF o x-RACF adyacente deberá desglosar dicha solicitud en componentes de medios (vídeo, audio, texto, etc.), cada uno de los cuales podrá tener un nivel de prioridad más o menos alto con respecto a otros medios dentro de la misma solicitud.

1.2.3. Arquitectura de referencia del 3GPP

El 3GPP es la entidad que ha especificado las tecnologías más importantes de telefonía móvil desde GPRS pasando por UMTS y acabando en LTE. En la figura 10 se puede apreciar la arquitectura de referencia del modelo control de políticas que el 3GPP propone. Se llama Control de Políticas y Cargos (Policy Control and Charging o PCC) y permite a los operadores realizar control de políticas de QoS basados en servicio y control de cargos basados en flujos.

Figura 10. Arquitectura de referencia del PCC



Veremos primero conceptos clave así como la arquitectura funcional de la red de acceso y troncal de LTE (llamada Evolved Packet System) para posteriormente ver el modelo de referencia PCC con todos sus bloques y sus interfaces.

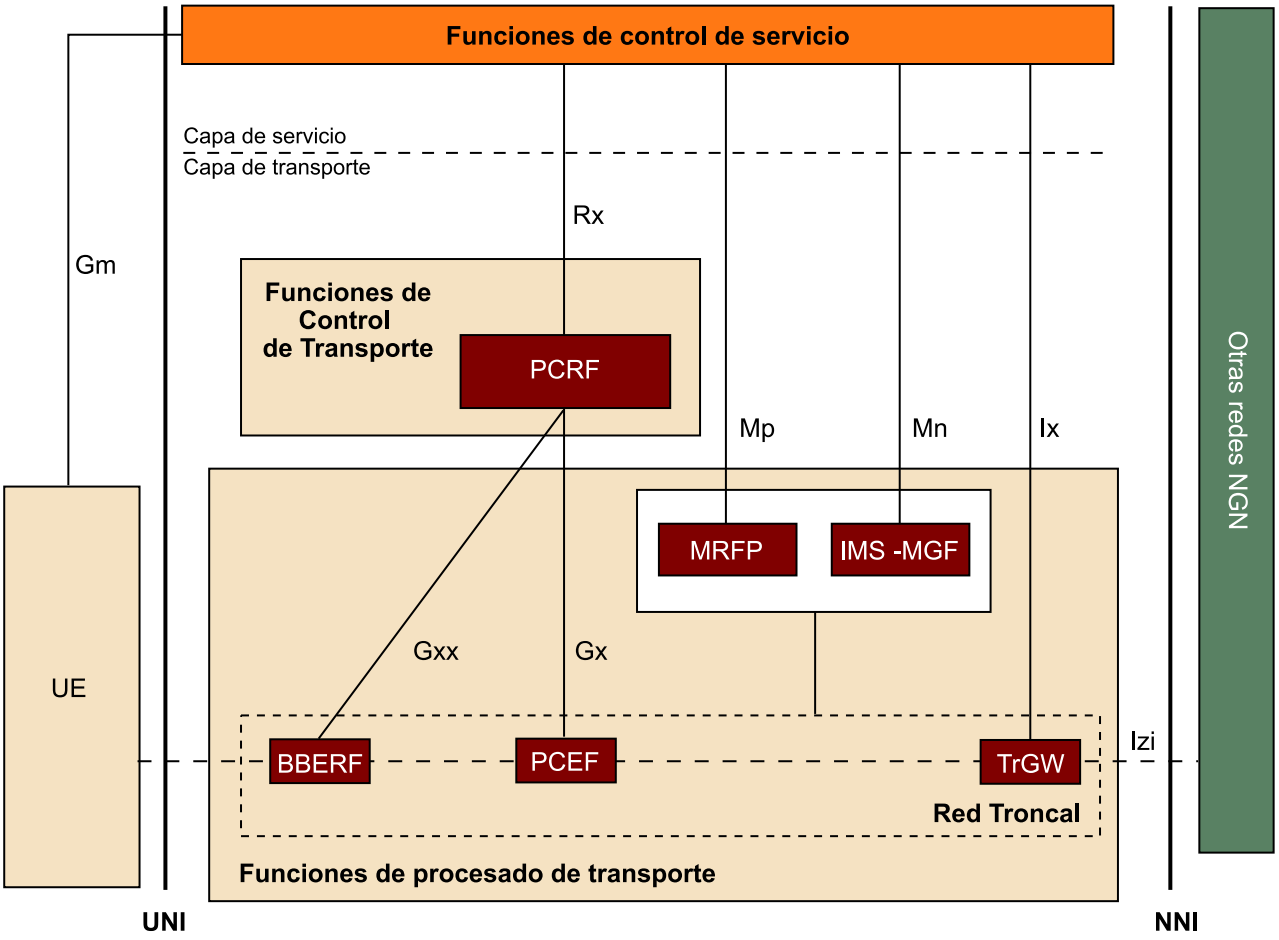
Ved también

Sobre los bloques e interfaces del modelo de referencia PCC, podéis ver un resumen explicativo en la tabla 9 del anexo.

El EPS 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.

En la siguiente figura podemos ver otras funciones de procesado de transporte aparte de las mostradas en la figura que muestra el modelo PCC.

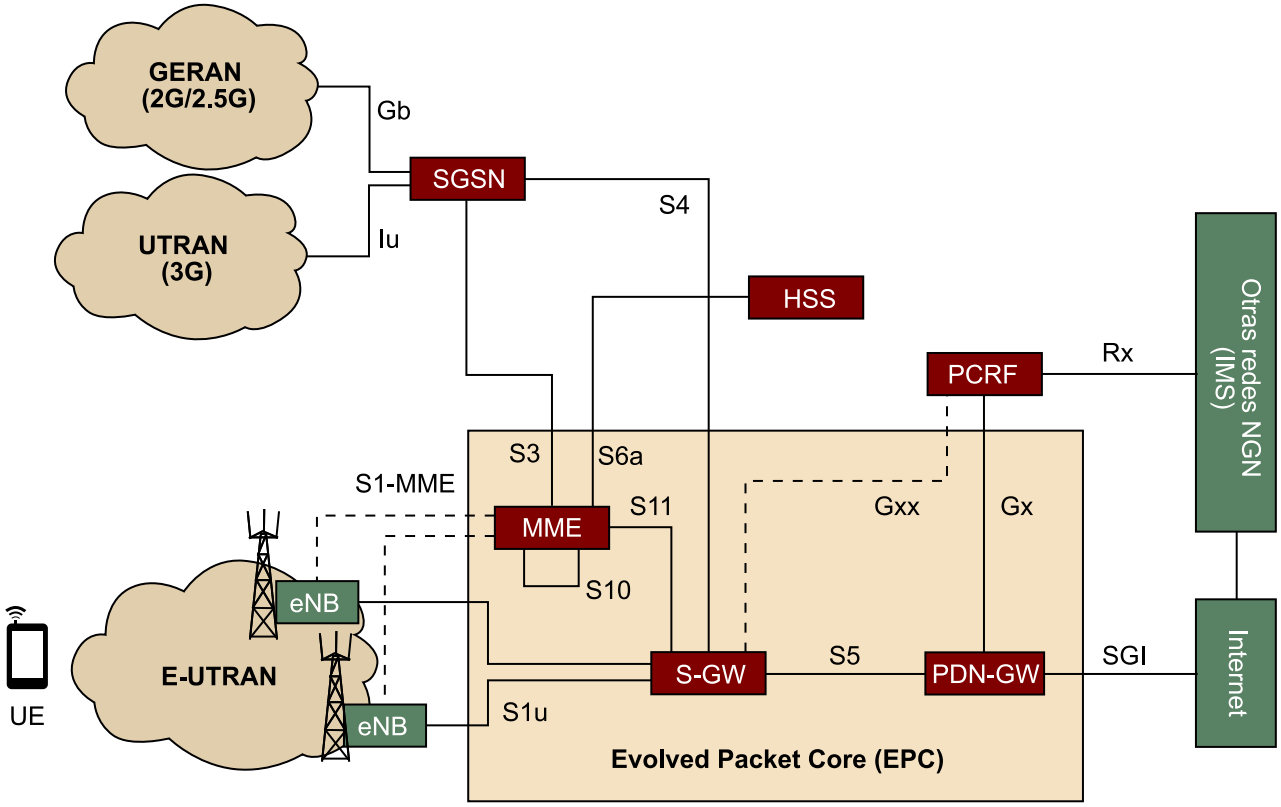
Figura 11. Otras funciones de procesado de transporte según 3GPP



Introducción al Evolved Paquet System

La figura 12 muestra la arquitectura del EPS o también llamado SAE (System Architecture Evolution). A continuación veremos los elementos que la componen.

Figura 12. Arquitectura de referencia de EPS



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 (no contempla *a priori* la existencia de una pasarela residencial con equipos conectados detrás). Esto tiene simplificaciones importantes en la arquitectura de procesado de transporte en la parte de la red de acceso.

Más allá del equipo de usuario está la red de acceso radio de LTE, que se llama E-UTRAN. Dicha red de acceso radio acaba en el eNodeB (Evolved Node B) que, para que nos entendamos, es la estación base de LTE. Este elemento define una serie de canales virtuales radio (basado en la tecnología OFDMA) 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 de transmisión radio, también llamados en inglés *radio bearers*.

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

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.

Nota

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).

El MME realiza otras funciones. Por ejemplo, aglutina información actualizada de localización de cada equipo de usuario (a qué eNodeB está asociado). Esto es importante cuando se produce una llamada entrante hacia un usuario (al servicio de localización se le llama *paging*) y hay que localizarlo. También realiza tareas de autenticación del equipo de usuario en el momento en que se produce la adhesión a la red. Es por ello por lo que el MME tiene un punto de referencia dedicado de interconexión al HSS (Home Subscriber Server) donde se almacena la información de credenciales del usuario y perfil de suscripción a nivel de transporte (y también a nivel de control de servicio). Finalmente, el MME también tiene tareas de gestión de *radio bearers*.

Para finalizar tenemos el último elemento del EPC, el PDN GW o Packet Data Network Gateway. Es el elemento fronterizo del sistema EPS con otras redes externas como Internet o IMS. Este elemento juega un papel muy importante en la garantía de QoS, como veremos más adelante. Esta entidad también se encarga de asignar las direcciones IP a los equipos de usuarios.

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

Para empezar vamos a definir el concepto de ***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 hasta la PDN GW y todo paquete IP que entre en dicho túnel gozará de un tratamiento a nivel de garantía de QoS especificas a lo largo de todo el EPC. A partir de ahora llamaremos al *EPS bearer*, el túnel EPS.

Nota

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 bearer*: *default bearer* y *dedicated bearer*.

Túnel EPS

Cuando un paquete IP llega al eNodeB, éste mapea el túnel EPS a una portadora rádio de características similares de QoS. Es muy importante entender que el mapeo que el eNodeB realiza entre un túnel EPS y una portadora rádio 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.

Así, un solo equipo de usuario puede tener más de un *IP-CAN bearer* (túnel IP-CAN a partir de ahora) establecido con la correspondiente PDN GW y cada uno tiene sus propias características de QoS. Los túneles IP -CAN pueden ser unidireccionales o bidireccionales y pueden ser establecidos, modificados o liberados por el propio equipo de usuario o por la red de acceso.

¿Qué parámetros define el 3GPP para caracterizar a nivel de QoS un túnel IP-CAN? El 3GPP ha definidos cuatro parámetros:

1) QoS Class Identifier: que define el comportamiento de QoS del tráfico asociado a un túnel IP-CAN.

Un QCI, o *QoS Class Identifier*, es un identificador que especifica 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 desde el equipo de usuario hasta la PDN GW) y tasa de pérdida de paquetes (la tasa de pérdida de paquete máxima deseada desde el equipo de usuario hasta la PDN GW). El 3GPP ha estandarizado 9 QCI, con valores asignados a los respectivos parámetros, para 9 tipos de servicios predefinidos.

2) Allocation and Retention Priority: este parámetro indica cuán importante (nivel de prioridad) es el túnel IP-CAN con respecto a otros túneles IP-CAN.

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 IP-CAN no se puede realizar porque no hay recursos suficientes? Pues hay que desalojar otros túneles IP-CAN 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: indica la cantidad garantizada de bits por segundo que se necesitan (capacidad reservada) para este túnel IP-CAN. Se usa solo para servicios en tiempo real. El GBR puede modificarse si se requiere una ampliación o disminución del volumen de tráfico a garantizar.

4) Maximum Bit Rate: indica la cantidad máxima de bits por segundo permitida (de pico) para este túnel IP-CAN. Se usa solo para servicios en tiempo real.

Así pues, el mecanismo que el EPS utiliza para garantizar la QoS está basado en estos túneles IP-CAN. Un equipo de usuario puede tener asignados varios túneles IP-CAN simultáneos dedicados con diferentes características de QoS.

Como curiosidad, tan pronto como un terminal móvil se enciende, el sistema le otorga automáticamente una dirección IP y un túnel IP-CAN bidireccional sin ninguna garantía de QoS ni GBR (pero sí con un MBR fijado según la suscripción del usuario), el cual lo mantiene hasta que se apaga. Este túnel IP-CAN es de tipo *default* y es establecido por la red de acceso (gestionado por el MME). A partir de ese momento el terminal o la red puede establecer túneles IP-CAN adicionales de tipo *dedicated*para garantizar la QoS de los servicios que se invoquen.

Tanto la PDN GW en sentido de bajada o *downlink* como el equipo de usuario en sentido de subida o *uplink* mapean los paquetes IP entrantes a unos filtros de paquetes IP llamados **flujos de datos de servicio**, y una vez identificado a qué flujo de servicio pertenece, se mapea al túnel IP-CAN asignado para garantizar la QoS.

Los **flujos de datos de servicio** se definen como un agregado de flujos de paquetes cada uno de ellos caracterizados por tener idénticas direcciones IP tanto de origen como de destino, y por los puertos usados y el protocolo.

El modelo de referencia PCC

El PCC trabaja a nivel de flujos de datos de servicios y proporciona funciones para el control de políticas y de facturación (cargos asociados) así como reporte de eventos para los flujos de datos de servicio. La funcionalidad del PCC se resume en dos funciones principales:

1) Facturación en base a flujos: en los que se encuentran el control de cargos asociados y el control de crédito *on-line*.
2) Control de políticas: en los que se encuentran control de acceso y control de QoS, entre otros.

Cada flujo de datos de servicio ha de venir 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** (definida por el PCRF tras tomar la decisión de control de admisión de la solicitud de recursos de servicio vía la interfaz Rx en modo *push* o desde la interfaz Gx en modo *pull*) está compuesta por los siguientes parámetros:

- Nombre de regla (identificador único)
- Identificador de servicio (valor entero que identifica un servicio o componente de servicio)
- Filtro(s) de flujos de datos de servicio (fija parámetros de cabecera del paquete TCP/IP para mapear el tráfico real al servicio)
- Precedencia (orden de aplicación de los filtros)
- Estatus de acceso (abierto o cerrado)
- Parametros QoS (contiene QCI, ARP y velocidad de bit para subida y bajada)
- Clave de facturación (es decir, *rating group*) y otros parámetros de facturación (usados para facturación *on-line y off-line*)
- Clave de monitorización

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 (en una interfaz llamada Rx) con una sesión IP-CAN a nivel de transporte (en una interfaz llamada *Gx/Gxx*).

Una sesión IP-CAN se caracteriza por ser la asociación entre el equipo de usuario y una red IP. Una sesión IP-CAN puede incorporar una agrupación de uno o más túneles IP-CAN. Una sesión IP-CAN está presente siempre que la dirección IP esté asignada al equipo de usuario y notificada a la red IP.

1) Subcapa de procesado de transporte

La figura 10 muestra dos elementos que conformarían 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. Aquí hemos incluido las dos entidades encargadas del control de cargos asociados: el OCS y el OFCS. Finalmente, describiremos las tres entidades funcionales de procesado de transporte restantes que aparecen en la figura 11, las cuales serán agrupadas en la red troncal

Reflexión

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.

a) Función de Aplicación de Políticas y Cargos Asociados (PCEF): En inglés se traduce a Policy and Charging Enforcement Function (PCEF) y esta entidad funcional se encarga de aplicar las políticas que definen las reglas PCC que uno o más PCRF le indiquen a través de punto de referencia Gx. Esto significa que define los túneles IP-CAN, limita la velocidad de bit que indica el bearer (GBR y MBR) y realiza filtrado de paquetes (inspección de paquetes IP de entrada desde las redes externas) según los filtros definidos por las reglas PCC activas para mapear el tráfico a los IP-CAN bearers adecuados para la QoS requerida. Además, mapea los IP-CAN bearers a parámetros de QoS concretos de la red troncal o EPC (DiffServ, básicamente).

La localización del PCEF en la arquitectura EPS es en el PDN GW. En el caso de una red GPRS, el PCEF se localizaría en la GGSN; en el caso de una red Wi-Fi sería la PDG.

Pasarelas

Todas estas pasarelas con distintos nombres guardan una similitud entre ellas. Son pasarelas fronterizas de la red de acceso con otras redes externas basadas en paquetes y administradas por otros operadores. Son las entidades funcionales encargadas de interconectar cada una de las redes de acceso radio con otras redes externas terrestres.

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 túneles IP-CAN, etc.) incluyendo funciones que afectan al reporte de eventos hacia el PCRF para notificar la modificación o el establecimiento de un túnel IP-CAN 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 *of-fline* ni será causa de consumo de crédito en la facturación *on-line*.

Las llamadas **reglas PCC** son en realidad el resultado de las decisiones a nivel de sesión que la entidad funcional PRCF (servidor de políticas en la subcapa de control de transporte) toma una vez ha evaluado información de disponibilidad de la red y políticas del operador de la misma red. Es una decisión de control de admisión a nivel de flujos de datos de servicio (cuya descripción es recibida desde el punto de referencia Rx) y las reglas PCC son el resultado de ésta.

Así pues, los flujos de datos de servicio (asociados a cada regla PCC en forma de filtros) también pueden estar sujetos a un control de facturación si el servicio al que va asociado así lo requiere. Así pues, el PCEF debe estar al corriente de dicho control también. De hecho el 3GPP ha definido dos interfaces dedicadas con las entidades funcionales OCS y OFCS con unos puntos de referencia llamados Gy y Gz respectivamente.

Por ejemplo, para el caso de tener un flujo de datos de servicio sujeto solo a control de facturación, el PCEF permite que un flujo de datos de servicio (definidos por una regla PCC activa) que esté sujeto a control de facturación pase a través de él si y solo 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 flujo de datos de servicio que está 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 solo 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 *on-line*, 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 solo si se cumplen las condiciones impuestas por la políticas correspondientes.

b) Función de Asociación de Túneles y Reporte de Eventos (BBERF): En inglés se llama *Bearer Binding and Event Reporting Function* y esta entidad funcional 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 también es capaz de mapear el tráfico a los túneles IP-CAN. Os preguntareis para qué el BBREF realiza esta función si el PCEF ya lo hace como extremo de túnel. Resulta 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 PRCF 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.

c) Sistema de Facturación Online (OCS): El Online Charging System realiza la gestión del crédito para la facturación de pre-pago. 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 éste 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 (velocidad del túnel IP-CAN de tipo *default*).

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.

e) Procesado de Funcionalidades de Recursos Multimedia (MRFP): Esta funcionalidad es equivalente a la descrita en el modelo del ETSI-TISPAN con el mismo nombre.

f) Funcionalidad de Pasarela de Medios de IMS (IMS-MGF): Esta funcionalidad es equivalente a la descrita en el modelo del ETSI-TISPAN con el nombre T-MGF.

g) Pasarela de Transición (TrGW): La Transition Gateway (TrGW) tiene funciones muy similares a la funcionalidad del I-BGF de la ETSI-TISPAN, ya descrita anteriormente. Está interconectada con la capa de control de servicio vía una interfaz llamada Ix.

2) Subcapa de control de transporte

En el modelo del 3GPP, esta subcapa está formada por dos elementos: SPR y PCRF.

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 admisión y generar las correspondientes reglas PCC.

Nota

Fijaos que si lo comparamos con los bloques dedicados a la adhesión de los terminales a la red de acceso de la ITU-T (llamado NACF) y de la ETSI-TISPAN (NASS), el SPR cumpliría solo con la función de interconexión entre el TLM-FE y el PD-FE dentro del RACF (vía la interfaz Ru) o entre el CLF y el A-RACF dentro del RACS (vía la interfaz e4).

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 Functions) 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 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 es el P-CSCF y si no está basado en IMS es una entidad equivalente.

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

- **Autorización de la propia solicitud de recursos de servicio y control de admisión de suscripción**: Al 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 del usuario que ha solicitado. En caso de que no se cumpla solo una de estas dos comprobaciones la sesión se rechaza.

- **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 flujos de datos de servicio 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.

- **Reporte de eventos**: El PCRF puede por ejemplo reportar eventos ocurridos en la capa de Transporte (status de túneles IP-CAN o sesiones IP-CAN)

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

El PCRF soporta la comunicación con otros PCRF 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: 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.

Reflexión

Tras ver la descripción del PCRF, podemos sacar la conclusión de que al compararlo con los elementos de control de admisión y recursos equivalentes para la ITU-T (RACF) y la ETSI-TISPAN (RACS), todos cumplen en general con funciones muy similares y que en lo único que se diferencian es por el desglose interno en entidades funcionales y cómo las funciones se reparten entre ellas.

1.3. Capa de servicio

En la capa de servicio no existen muchas divergencias entre entidades de estandarización ya que se trata de una capa que no guarda relación con ninguna tecnología en particular, como sí ocurría en la capa de transporte.

No obstante, cada entidad de estandarización ofrece su punto de vista y perspectiva particular respecto a esta capa:

- 3GPP: como entidad creadora del IMS, centra su arquitectura de control de servicio en esta tecnología.

- ITU-T: en su recomendación Functional Requirements and Arquitecture (FRA), especifica un modelo funcional genérico del plano de servicios que pretende ser independiente de los servicios y protocolos empleados. De esta forma, este modelo puede concretarse en modelos más específicos, conocidos como **componentes de servicios** (de los cuales se extrae el componente IMS, el de emulación RTC/RDSI y el de IPTV).

- ETSI-TISPAN: presenta un enfoque orientado a **subsistemas**. Cada subsistema tiene su propio modelo de arquitectura y se especifica independientemente de los otros subsistemas. De esta forma pueden añadirse con el tiempo nuevos subsistemas que cubran nuevas demandas y clases de servicio, y permite la importación y adaptación de subsistemas ya definidos, como es el caso de IMS. Aparte del de IMS, el modelo de ETSI-TISPAN define dos subsistemas más: el de emulación RTC/RDSI y el de IPTV.

De todos estos componentes (ITU-T) y subsistemas (ETSI-TISPAN) hay uno que queremos destacar: el componente, subsistema o núcleo IMS.

El **núcleo IMS** aguanta la provisión de cualquier servicio multimedia existente hoy y también los futuros que están por llegar. IMS puede soportar la provisión de servicios equivalentes a las redes RTC/RDSI e incluso el servicio IPTV.

Cuando se define un servicio multimedia en redes NGN se suele distinguir entre que esté basado en IMS (participación de núcleo IMS con señalización SIP) o que no lo esté (con un componente o subsistema dedicado, el cual tiene sus propios bloques de control de servicio y su propio protocolo de señalización de servicio). Esto ocurre ya con otros componentes o subsistemas separados que la especificación de redes NGN contemplan como el de emulación RTC/RDSI y el de IPTV. Así, las entidades de estandarización de las redes NGN a nivel de servicio dejan la puerta abierta a la especificación de dichos servicios sin que tengan que estar basados en IMS.

Así pues, nos vamos a centrar exclusivamente en el núcleo IMS como plataforma de provisión y habilitación de servicios multimedia.

Como las especificaciones del componente o subsistema IMS de la ITU-T y de la ETSI-TISPAN están basadas en el estándar del 3GPP, vamos a intentar dar una descripción más uniforme de este subsistema haciendo hincapié en las diferencias entre especificaciones de una u otra entidad de estandarización tomando como base la del 3GPP.

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) a los que acceden a través del núcleo IMS.

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 (como son la presencia y *push to talk* sobre entornos móviles), 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 IMS a un nivel superior. No obstante, en ellos recae la provisión de la mayoría de los servicios que aportan valor a 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.

1.3.1. Componentes del núcleo IMS

Siguiendo la línea de anteriores apartados vamos a hacer un repaso por las tres especificaciones que venimos analizando: 3GPP, ETSI-TISPAN y ITU-T. En las siguientes figuras se muestran las tres arquitecturas funcionales para cada una de ellas. Sin embargo, dada la gran similitud entre sí, vamos a dar una única explicación descriptiva, la del modelo 3GPP, mencionando las diferencias que pueda haber con las dos restantes: ITU-T y ETSI-TISPAN.

Ved también

Un resumen conjunto de las interfaces que componen los tres modelos de IMS se puede encontrar en la tabla 10 del anexo.

Figura 13. Arquitectura de referencia del componente IMS para ITU-T

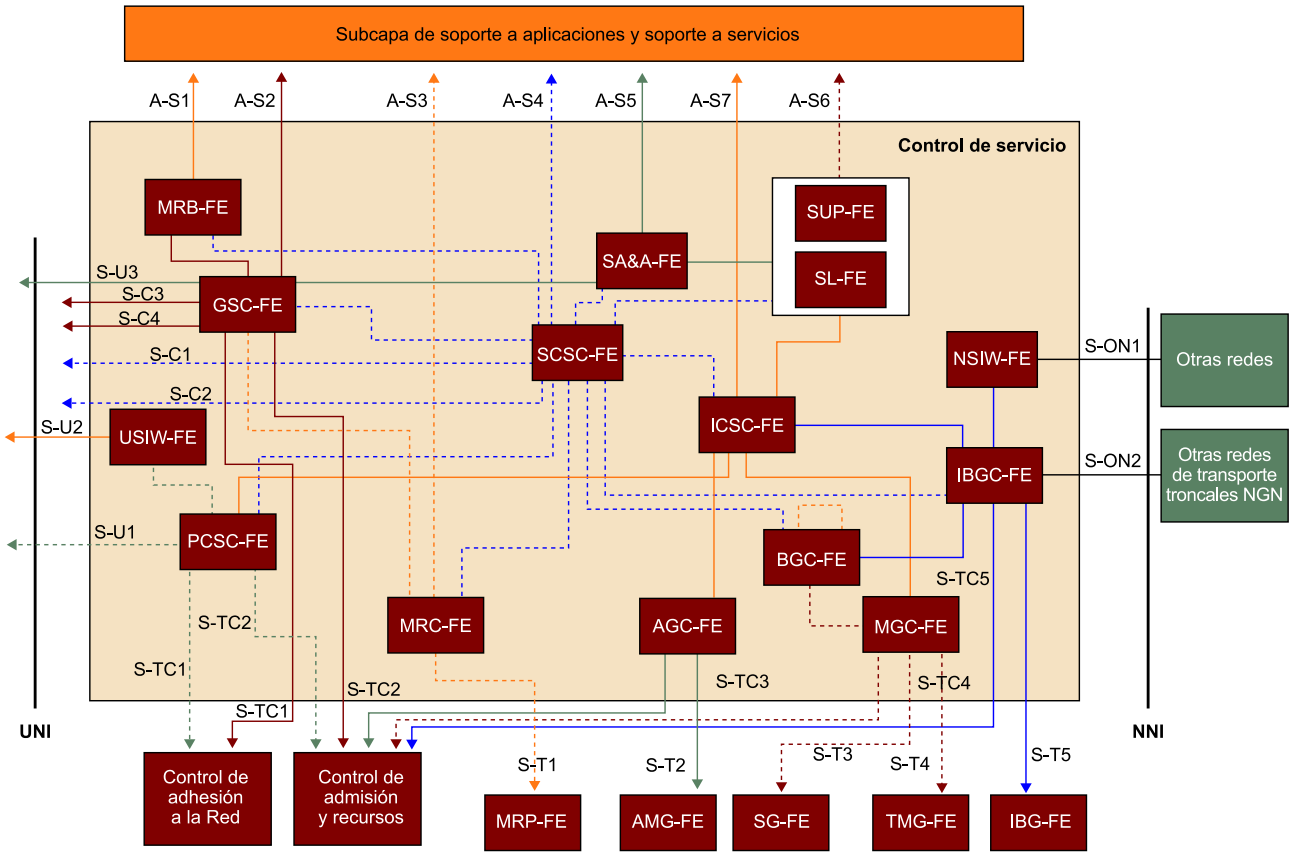


Figura 14. Arquitectura de referencia para el subsistema IMS para la ETSI-TISPAN

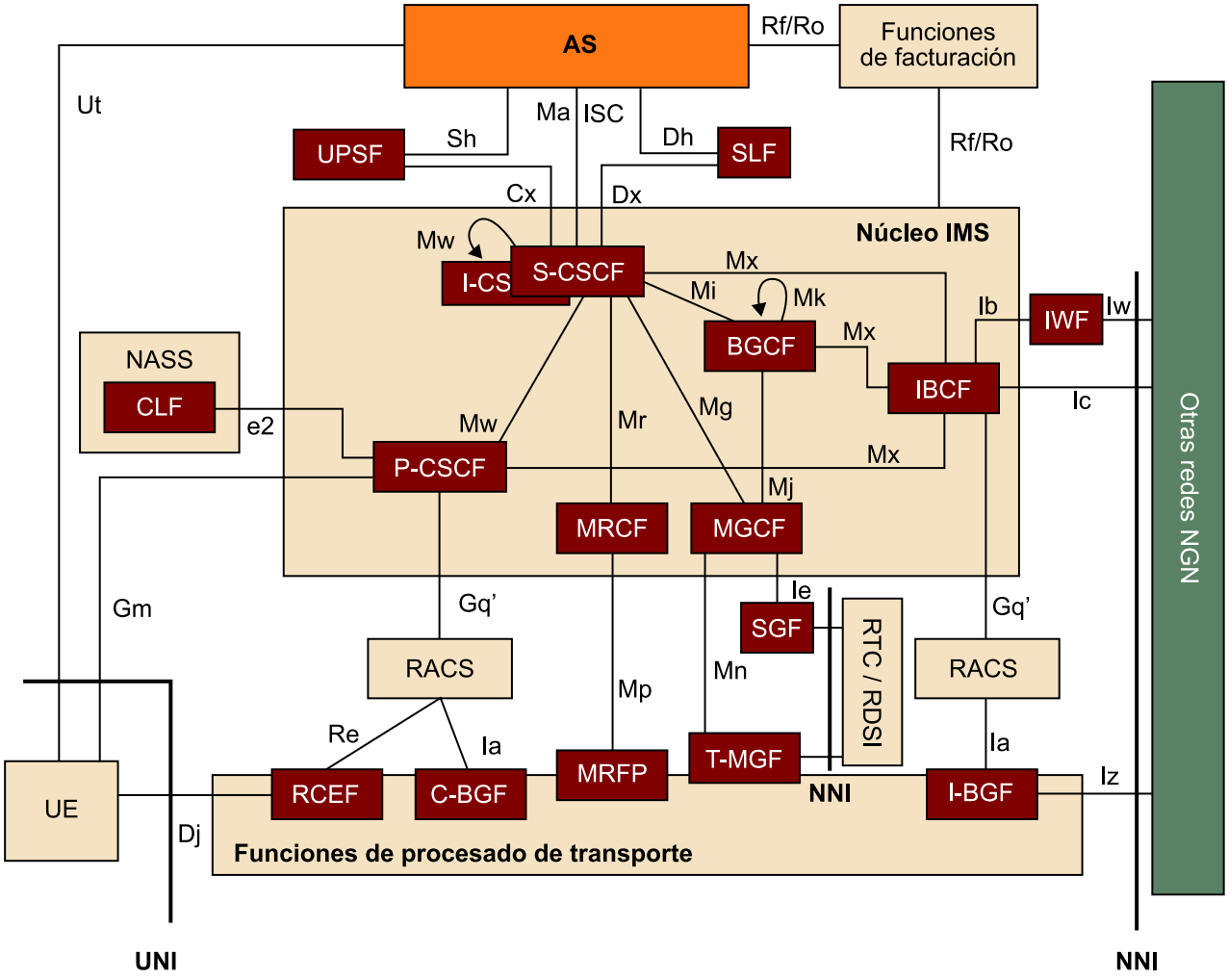
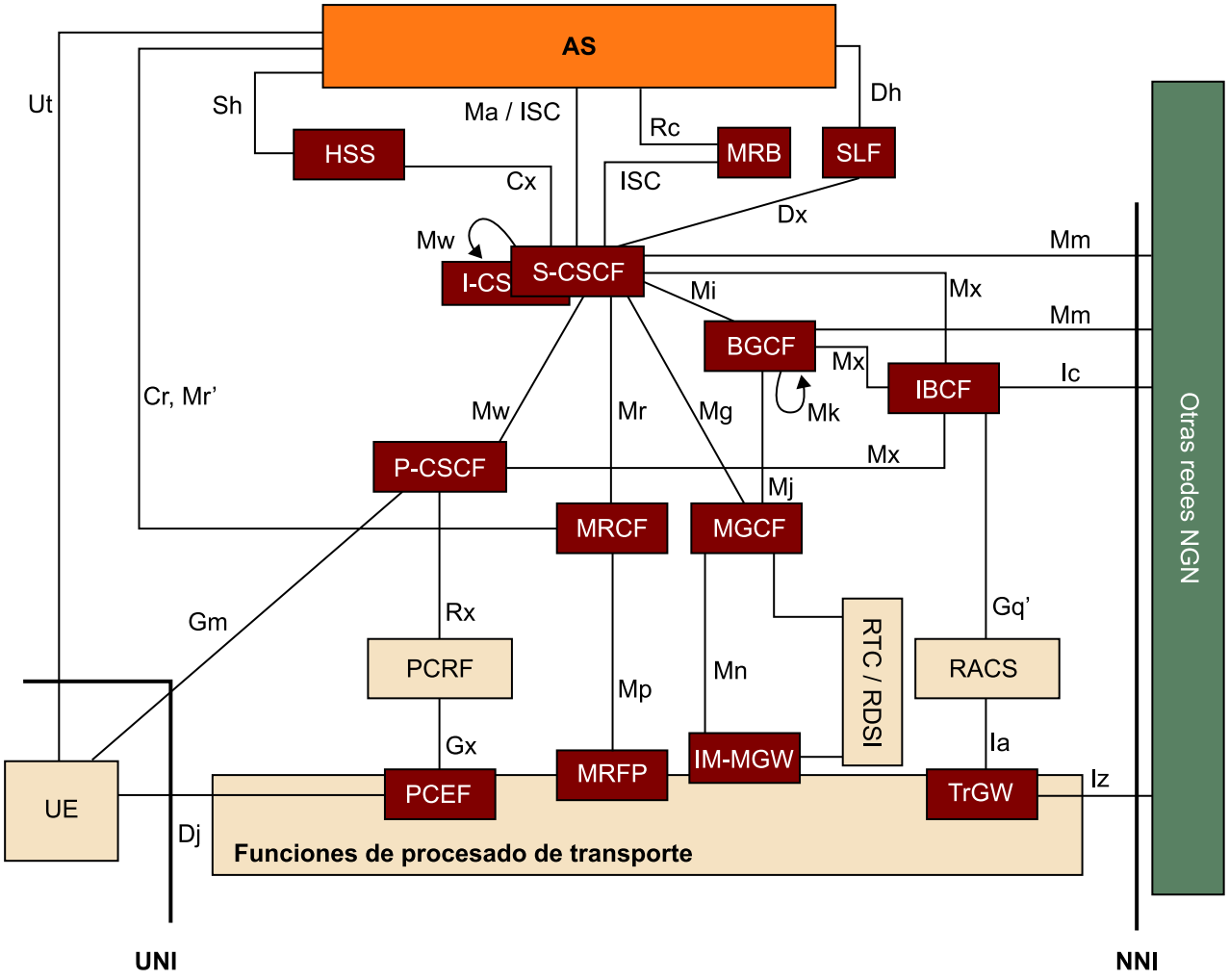


Figura 15. Arquitectura de referencia de IMS para 3GPP



Tanto en la figura 14 como en la figura 15, las entidades S-CSCF y I-CSCF se han mostrado juntas para simplificar el diagrama, pero en realidad son dos entidades completamente independientes. Ambas están interconectadas a través de la interfaz Mw. Pero además, cada interfaz que sale del S-CSCF debe ser replicada también para el I-CSCF (exceptuando la Mr y Mi, que solo están asociadas al S-CSCF). La interfaz que conecta el S-CSCF con el AS es la ICSy la que conecta al I-CSCF con el AS es la Ma.

El protocolo utilizado en el establecimiento de sesiones de servicios multimedia basados en IMS es el protocolo SIP (Session Initiation Protocol) definido por el IETF en el RFC 3261. No obstante, el protocolo SIP requiere de ciertas extensiones que van más allá de la especificación del IETF para ser usado en un entorno IMS.

Ved también

Las extensiones del protocolo SIP están descritas en el subapartado "Extensiones para IMS".

Función de Control de Sesión de Llamada – Proxy (P-CSCF)

El P-CSCF es el primer punto de contacto dentro de IMS para los usuarios adheridos a una red de acceso y es por ello por lo 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 equipo de usuario 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 separadas para señalización y medios.

Entre las funciones que ha de realizar el P-CSCF están las siguientes:

a) En el proceso de registro del usuario, reenviar la petición de SIP REGISTER desde el UE (recibida vía una interfaz llamada *Gm*) al punto de entrada del dominio local. Mirando la parte que describe el dominio en el SIP URI incluido en la cabecera SIP sabe a qué I-CSCF (servidor de control de sesión de llamada de tipo *Interrogating*) ha de reenviar al SIP REGISTER.

Nota

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).

b) Almacenar información del registro, como la información de contacto del UE (IP asignada), la dirección del S-CSCF (servidor de control de sesión de llamada de tipo *Serving*) y las sesiones en activo.

c) Redirigir los mensajes SIP desde el UE al S-CSCF vía una interfaz llamada *Mw*, y viceversa.

d) Realizar la compresión y descompresión de los mensajes SIP que provienen del UE.

El UE, al enviar sus mensajes SIP por la interfaz de señalización de IMS llamada Gm, pondrá siempre la dirección IP del P-CSCF como destino, ya que éste hace de proxy para todas las transacciones SIP.

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

Cuando el P-CSCF recibe un intento de llamada (SIP INVITE) (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 pre-configurada de teléfonos de emergencia (normalmente es la misma lista independientemente del país gracias acuerdos internacionales, como el número 112).

f) La asociación entre el P-CSC-FE y cada UE es siempre segura (usando IPSec). Por lo tanto, el P-CSCF es responsable del mantenimiento de las Asociaciones de Seguridad (SA-Security Associations) y la aplicación de la protección de confidencialidad e integridad de señalización SIP.

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.

g) Participa en la autorización y la gestión de calidad de servicio de los recursos multimedia (se comunica con la subcapa de control de transporte para solicitar recursos vía la interfaz Rx). Es normal que al ser un SBC tenga que consultar elementos de gestión de recursos en la capa de transporte.

El P-CSCF recibe todas las peticiones SIP que hacen los UE en su dominio, independientemente del destino final de éstas, y las reenvía a un I-CSCF o un S-CSCF de su mismo dominio para que continúe su procesado. Asimismo, recibe todas las peticiones SIP destinadas a los UE de su dominio. El P-CSCF ha de mantener información de registro y de estado.

Dentro de la red de un operador pueden existir varios P-CSCF de forma concurrente.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- La interfaz e2 aparece para conectarse con el NASS.
  El P-CSCF puede obtener la dirección del elemento que gestiona los recursos en la capa de transporte gracias a la información de localización del usuario proporcionada vía la interfaz e2. En el modelo del 3GPP no se usa porque está basado en túneles IP-CAN.

- La interfaz Rx pasa a llamarse Gq' y le conecta al RACS en vez del PCRF.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- El nombre de esta entidad (P-CSCF) cambia a P-CSC-FE.

- La interfaz Gm pasa a llamarse S-U1 y también está basado en SIP. Cabe destacar también que la ITU-T incluye una entidad llamada User Signalling Interworking Functional Entity (USIW-FE) que implementa una interfaz llamada S-U2 con el equipo de usuario (UE) y otra interfaz con el P-CSC-FE (podría ser equivalente al Gm o S-U1) y su función es adaptar o traducir la señalización de todos aquellos terminales de usuario que no soportan el protocolo SIP de IMS.

- La interfaz e2 (ETSI-TISPAN) pasa a llamarse S-TC1 con la misma función que éste.

- La interfaz Rx pasa a llamarse S-TC2 (o Rs) y le conecta al bloque de control de admisión y recursos de la subcapa de control de transporte (RACF) en vez del PCRF.

Función de Control de Sesión de Llamada – Interrogating (I-CSCF)

I-CSCF es el punto de contacto dentro de la red del operador para todas las conexiones destinadas a un subscriptor de este operador de red.

Veamos las cuatro funciones asignadas al I-CSCF:

a) Obtener el nombre del siguiente salto (S-CSCF o AS) desde el HSS vía la interfaz Cx.

b) Asignar un S-CSCF en función de las capacidades recibidas desde el HSS. La asignación del S-CSCF tendrá lugar cuando un usuario se registra en la red. También se asigna un S-CSCF cuando recibe una petición SIP mientras no está registrado en la red, pero en cambio tiene servicios relativos a un estado de no registrado (por ejemplo, mensajes de voz).

c) Encaminar las peticiones SIP de entrada en relación con un S-CSCF asignado (vía la interfaz Mw) o con un AS (vía una interfaz llamada Ma).

d) Proporcionar funcionalidad THIG (Topology Hiding Inter-network Gateway) de manera opcional. Otro operador que quiera enviar señalización SIP hacia mi dominio, lo enviará al I-CSCF como si fuera un proxy, ya que será el único elemento del núcleo IMS visible desde el exterior. El I-CSCF puede actuar como un elemento SBC solo a nivel de señalización SIP para la interfaz entre dos dominios o redes NGN (NNI). No obstante, no contempla gestión de recursos con la capa de transporte.

Nota

En el Release actual del 3GPP el IBCF ha sustituido esta funcionalidad de THIG al I-CSCF. No obstante, se pueden encontrar aún numerosos documentos que describen flujos de llamadas IMS en las que el I-CSCF es el elemento visible entre distintos dominios IMS.

En el caso de tramitación de un registro de usuario, el I-CSCF contacta con la base de datos de suscriptores del dominio o HSS (vía una interfaz llamada Cx) para obtener la dirección del S-CSCF, y entonces reenvía el mensaje SIP a dicho S-CSCF vía la interfaz dedicada a tal fin, llamada Mw. Esta operación se realiza de la siguiente manera: el I-CSCF contacta con el HSS para realizar el registro, ésta autoriza dicho registro y, a través de la interfaz Cx, basada en el protocolo Diameter, el I-CSCF solicita y selecciona en una lista del HSS, el primer servidor que satisface las capacidades requeridas.

Aparece una interfaz llamada Mm, que, según el 3GPP, es una interfaz IP entre los CSCF/IBCF y otras redes IP para, por ejemplo, recibir una petición de sesión desde otro servidor SIP o terminal.

Reflexión

El estándar del 3GPP no da mucha más información sobre la inclusión de esta interfaz Mm. Esta interfaz está basada en SIP y sirve para comunicarse con otros servidores SIP externos.

Para la recepción de los mensajes destinados al I-CSCF, deben habilitarse puertos específicos. El I-CSCF no mantiene ningún tipo de información de registro o estado. Múltiples I-CSCF pueden existir concurrentemente en la red de un operador.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- La entidad HSS pasa a llamarse User Profile Subscription Function(UPSF).
- La interfaz Mm no existe.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- El nombre de esta entidad (I-CSCF) cambia a I-CSC-FE.
- La entidad HSS pasa a llamarse Service User Profile Functional Entity (SUP-FE).
- La interfaz Mm no existe.

Función de Control de Sesión de Llamada - Serving (S-CSCF)

El S-CSCF es el punto central del núcleo IMS y el dominio correspondiente siendo 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.

Cuando un usuario envía una petición de registro (SIP REGISTER), ésta se envía al S-CSCF (desde el I-CSCF vía la interfaz Mw), el cual descarga los datos de autenticación desde el HSS (vía la interfaz Cx). Después de este procedimiento de registro, el usuario puede iniciar y recibir servicios IMS. Finalmente, el S-CSCF descarga del HSS un perfil de servicio del usuario como parte del proceso de registro.

Este perfil incluye las iFC o initial Filter Criteria, las cuales se usan para decidir qué servidores de aplicaciones (AS) están habilitados cuando un usuario envía una petición SIP. 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).

Para el tráfico SIP entrante en el dominio hacia un equipo de usuario (UE), el S-CSCF encamina las sesiones al P-CSCF, cuya dirección se almacenó durante el registro. En el caso del tráfico saliente, el S-CSCF pregunta al DNS/ENUM para determinar la ruta de la llamada. Es decir, encamina el mensaje hacia el IBCF (elemento fronterizo entre dominios IMS) que le conecta con el dominio destino. El S-CSCF ha de ser capaz de encaminar basándose en formatos SIP URI o Tel URI. En este último caso, el mensaje SIP se encaminará hacia una entidad que gestiona estos tipos de URI de destino, el Breakout Gateway

Control Function o BGCF. Éste, al ver que es de tipo Tel URI, lo reenviará a un Media Gateway Control Function o MGCF (pasarela de control hacia RTC/RDSI) de su elección.

Se han de definir puertos específicos para la recepción de mensajes en el S-CSCF. El S-CSCF ha de mantener tanto el estado del registro como el de la sesión. Múltiples S-CSCF pueden existir concurrentemente en la red de un operador.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- La interfaz Mm desaparece.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- El nombre de esta entidad (S-CSCF) cambia a S-CSC-FE.

Función de Control de Sesión de Llamada – Emergency (E-CSCF) y Función de Obtención de Localización (LRF)

Estas entidades no han sido incluidas en la figura 15 para no complicar más la arquitectura pero hemos creído conveniente incluir su descripción, ya que, de acuerdo con la normativa de la mayoría de los países, todo operador de telecomunicaciones debe proporcionar comunicaciones de emergencia y el E-CSCF se ha definido para tal fin, junto con el LRF, que realiza funciones de obtención de localización auxiliar.

La E-CSCF puede formar parte de un módulo único CSCF o funcionar como una aplicación independiente. En este último caso, se relaciona solo con el P-CSCF vía la interfaz Mw basada en señalización SIP.

El funcionamiento de esta entidad es el siguiente:

- Cuando el P-CSCF recibe un intento de llamada (SIP INVITE), el número de teléfono (Tel URI) se compara con una lista pre-configurada de teléfonos de emergencia.

- Si hay una coincidencia, la llamada se encamina con máxima prioridad (no se aplica control de cargos o facturación) y se envía a la E-CSCF para que la procese.

- La E-CSCF comprueba si hay información de localización (cabecera PANI – P Access Network Info) en el mensaje. Si no la hay, trata de obtenerla de la HSS (en su caso, con intervención del nodo SLF).

- A continuación, si se ha configurado un nodo LRF, obtiene de éste el número de un centro de emergencia (Public Safety Answering Point o PSAP), adecuado a la información de localización proporcionada, y redirige la llamada hasta el mismo (con la intervención de un gateway MGC en caso de ser necesario).

Función de Control de Pasarela de Salida (BGCF)

El BGCF (Breakout Gateway Control Function) se emplea para seleccionar el siguiente salto (pasarela capaz de encaminar) de una petición SIP (recibida desde un I/S-CSCF vía una interfaz dedicada llamada Mi) cuando ésta está destinada a un alias que no puede ser traducido como un SIP URI (por ejemplo, es el caso de un Tel URI). La selección de esta pasarela se realiza en base al número de teléfono del usuario llamado, y si es posible, también del llamante. El alias de destino puede ser especificado por un equipo de usuario (UE) o un servidor de aplicacion (AS).

En el caso de llamadas hacia la RTC/RDSI (alias de destino es un Tel URI), el BGCF reenviaría la señalización de sesión SIP a un Media Gateway Control Function (MGCF) que él mismo selecciona vía una interfaz llamada Mj (si está en el mismo dominio) o una interfaz llamada Mk (si está en otro dominio), mientras que tratándose de llamadas hacia otros dominios IMS, se enviarían vía la interfaz llamada Mx a un Interconnection Border Control Function o IBCF.

El BGCF implementa otras capacidades adicionales, como redundancia (posibilidad de seleccionar otro BGCF en caso de que éste fallase) o enrutamiento basado en minimización de coste (hacia la pasarela más cercana a la red final).

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- La interfaz Mx se usa también para encaminar llamadas hacia redes H.323 u otros protocolos a un IBCF/IWF que la gestionaría.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- El nombre de esta entidad (BGCF) cambia a BGC-FE.

- La interfaz que comunica el BGC-FE con IBGC-FE se usa también para encaminar llamadas hacia redes H.323 u otros protocolos a un IBC-FE / NSIW-FE (Network Signalling Interworking Functional Entity) que la gestionaría.

Función de Control de Interconexión Fronteriza (IBCF)

El elemento funcional IBCF (Interconnection Border Control Function) hace la tarea principal de interconectar núcleos IMS pertenecientes a distintos operadores (es un elemento de tipo SBC). Este bloque hace un traspaso de la señalización SIP que recibe desde los CSCF a través de las interfaces Mx hacia otra entidad IBCF perteneciente al otro dominio. Este IBCF estará conectado con el IBCF del operador remoto a través de una interfaz llamada Ici, que está basada en SIP.

Puede realizar tareas de THIG u ocultación en las cabeceras SIP de información que pueda dar pistas sobre la topología del núcleo IMS (reescritura del campo *Record Route:* de la cabecera SIP). A través de la interfaz Ici pasará toda la señalización SIP de establecimiento de sesión entre los dos núcleos IMS.

La funcionalidad del IBCF abarca también lo siguiente:

- Realiza funciones de control fronterizo (SBC) en la capa de transportevía la interfaz de control Ix con la entidad TrGW (Transition Gateway, en la subcapa de procesado de transporte). Ésta aplica sobre el tráfico de usuario las traducciones de NAT, control de acceso y/o conversiones de IMS ALG (IPv4/IPv6) que le indica por esta interfaz. Existe una interfaz llamada *Izi* (en la subcapa de procesado de transporte) que interconecta dos TrGW de distinto dominio para transferirse flujos de medios entre ellos.

- Realiza funciones de IMS ALG (Application Level Gateway) para la traducción de IP (a nivel de cabecera SIP como SDP) entre sesiones IMS basadas en IPv4 a sesiones IMS basadas en IPv6 y viceversa.

- Explora la información de señalización basada en fuente/destino, más allá de la ya realizada en cada subsistema.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- El IBCF controla el I-BGF de la subcapa de procesado de transporte vía la interfaz que lo conecta con la subcapa de control de transporte representado por un RACS (Gq').

- El IBCF inserta el IWF en la señalización de la ruta cuando hay necesidad de interacción entre perfiles SIP diferentes o protocolos diferentes (por ejemplo, SIP y H.323 o SIP estándar de IETF y SIP con extensiones IMS). En este caso, el IWF actúa como un punto de entrada a la red IMS.

- El IBCF se comunica con otro IBCF homólogo a través de una interfaz llamada Ic (el Ici, que hemos mencionado antes, es una implementación especial del Ic) para intercambiarse señalización SIP.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- El nombre de esta entidad (IBCF) cambia a Interconnection Border GW Control – Functional Entity (IBGC-FE).

- A la hora de realizar la solicitud de reserva de recursos, el IBCF-FE se comunica con el RACF vía la interfaz Rs, y éste a su vez selecciona y controla el IBG-FE vía la interfaz Rw.

Gestor de Recursos de Medios (MRB)

El Media Resource Broker (MRB) gestiona un grupo heterogéneo de recursos MRF a compartir entre un grupo heterogéneo de servidores de aplicaciones (AS). Asigna recursos del servidor de medios a las llamadas a petición de los AS. Para ello emplea métodos y algoritmos que le ayudan a determinar cómo realizar esa asignación; y recopila información sobre la operatividad o no de un determinado servidor de medios, o su nivel de carga en caso de que esté operativo, a fin de seleccionar el más adecuado en cada momento. Tiene una interfaz llamada Rc con el AS y una interfaz llamada ISC (IMS Service Control) con el S-CSCF.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- La entidad equivalente al MRB no existe en este modelo de referencia.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- El nombre de esta entidad (MRB) cambia a Media Resource Broker Functional Entity (MRB-FE).
- La interfaz Rc pasa a llamarse A-S1.

Aunque está localizado en las funciones de control de servicios, el MRB-FE puede ser visto como parte de las funciones de la subcapa de soporte a servicios y soporte de aplicaciones (ver la figura 1).

Control de Funciones de Recursos Multimedia (MRFC)

El Multimedia Resource Function Control (MRFC) es un nodo de señalización que actúa ante el S-CSCF como Agente de Usuario SIP (terminal SIP), y que controla el MRFP (Multimedia Resource Function Processor) a través de una

interfaz llamada Mp. Interpreta las demandas procedentes del servidor de aplicación (AS) vía el S-CSCF (interfaz Mr) y controla el MRFP consistentemente para ofrecer los servicios que ofrece éste: IVR, anunciamientos, etc.

Tiene otras interfaces que le conectan directamente con el AS para que estos accedan a los recursos multimedia sin tener que pasar a través del S-CSCF (vía el MRB). La interfaz llamada Cr es utilizada por el AS para controlar los medios y la Mr' (basada en SIP) para controlar la sesión en el uso de dichos recursos.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- Las interfaces Cr y Mr' desaparecen.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- El nombre de esta entidad (MRFC) cambia a Multimedia Resource Control Functional Entity (MRC-FE).
- La interfaz de interacción con el MRP-FE es la S-T1.

Función de Control de Pasarela de Medios (MGCF)

La Media Gateway Control Function (MGCF) permite controlar un IMS-MGF (en la subcapa de procesado de transporte) a través de la interfaz Mn. También está directamente conectada a nivel de traducción de la mensajería SIP de establecimiento de sesión a señalización SS7/ISUP con la red RTC/RDSI y viceversa.

Este control incluye la asignación y liberación de recursos de la pasarela de medios, así como la modificación de tales recursos. El MGCF se comunica con el CSCF vía el BGCF (Breakout Gateway Control Function) a través de la interfaz Mj por un lado y las redes de conmutación de circuitos por otra (a través de las entidades de la subcapa de procesado de transporte).

Para llamadas entrantes desde las redes de conmutación de circuitos, el MGCF reenvía los mensajes SIP equivalentes al S-CSCF vía una interfaz llamada Mg. Con lo cual, dependiendo de la dirección de la llamada, utiliza la interfaz Mj (llamada saliente hacia RTC/RDSI) o la Mg (llamada entrante hacia IMS).

Para el caso del 3GPP, el MGCF aparece como elemento dentro de la propia arquitectura de IMS interconectando las redes basadas en circuitos.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- El MGCF está interconectado con el Signalling Gateway Function o SGF (en la subcapa de procesado de transporte) para permitir la interoperabilidad entre SIP y señalización SS7 vía una interfaz llamada Ie.
- El T-MGF es el equivalente al IMS-MGF del 3GPP.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- Esta entidad (MGCF) pasa a llamarse Media Gateway Control Functional Entity (MGC-FE).
- La interfaz de conexión entre el MGC-FE y el TMG-FE (equivalente al T-MGF de la ETSI) es la S-T4 en lugar de la Mn.
- La interfaz de conexión entre el MGC-FE y el SG-FE (equivalente al SGF de la ETSI) es la S-T3 en lugar de la Ie.
- Las funciones que realiza el MGCF se pueden mapear a la entidad equivalente en el modelo de la ITU-T: el Network Signalling Interworking Functional Entity (NSIW-FE).

1.3.2. 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. En total hay 2 entidades y las interfaces involucradas están resumidas en la tabla 11 del anexo.

Servidor de Perfiles Local (HSS)

En IMS, la base de datos HSS (Home Subscriber Server) mantiene la relación entre las diferentes identidades (privada, pública…), almacena los perfiles de usuario y los distribuye a las entidades de red que controlan las sesiones de usuario (CSCF). Asimismo, es capaz de manejar distintos identificadores públicos de servicio (PSI) de acuerdo con las especificaciones de 3GPP.

Un **PSI (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. Puede identificar también por ejemplo a todo un grupo de usuarios.

El perfil de usuario tiene que incluir 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.

La HSS participa en los procedimientos de registro, re-registro y de-registro de usuario; registro implícito y manejo de sesión.

- El usuario inicia un proceso de registro (enviando mensaje SIP REGISTER) para informar a la red de su localización y capacidad para participar en una sesión. Durante este proceso se le asigna un S-CSCF (entidad de control de sesión de tipo *Serving*). 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, en los datos de configuración de la HSS y en la información de usuario almacenada. La HSS permite el proceso de asignación de S-CSCF comunicándole al I-CSCF (entidad de control de sesión de tipo *Interrogating*) 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. La HSS almacena la información del S-CSCF asignado.

- El re-registro es un proceso periódico iniciado por el equipo de usuario para refrescar el registro actual, o bien para cambiar el estado de registro del equipo de usuario (UE). El papel de la HSS en el re-registro es similar al del registro.

- Como resultado del de-registro el usuario deja de estar disponible con la identidad pública (IMPU) de-registrada. Éste puede ser solicitado por el usuario, iniciado por la red mediante un comando en la HSS o debido a un *time-out*.

- El procedimiento de registro implícito permite a un usuario registrarse y de-registrarse con un conjunto de identidades públicas (IMPU) identificando solo una de ellas en la petición de registro. El usuario es informado del resto de sus identidades como respuesta a la petición, de modo que estén disponibles más adelante para el manejo de la sesión.

- La HSS participa asimismo en el establecimiento de la sesión cuando el usuario la inicia (enviando mensaje SIP INVITE). La HSS devuelve al I-CSCF la identidad 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 no, la HSS tiene servicios para estado no registrado. Si la identidad pública no está registrada, y el usuario no tiene servicios para no registrados, la HSS indica al I-CSCF que el usuario no es alcanzable.

Junto con otros procedimientos de red, la HSS realiza la autenticación del usuario. La HSS debe soportar diversos modelos de autenticación: IMS AKA, IETF HTTP Digest e IMS SSO.

- El procedimiento de IETF HTTP Digest es el siguiente: la HSS genera uno o más tests de autenticación relativos al perfil de usuario, y los incluye en la respuesta al S-CSCF en el registro. El S-CSCF envía este test al usuario. La aplicación cliente genera la respuesta adecuada al mensaje (para lo que puede ser necesario que el usuario introduzca su *password*). El S-CSCF transfiere esta información a la HSS, que es entonces la encargada de verificar la respuesta.
- La autenticación IMS SSO permite que un usuario que ya tenga acceso a la red IP a través de la infraestructura del núcleo del operador no necesita autenticarse de nuevo para acceder al dominio IMS.
- Por su parte, IMS AKA permite la autenticación mutua del usuario y la red IMS, ofreciendo plena protección del tráfico de señalización en ambos sentidos.

La HSS también debe soportar la suscripción y notificación de cambios: los servidores de aplicaciones podrán suscribirse a notificaciones para la actualización de datos transparentes y no transparentes para un determinado usuario. El operador podrá configurar una lista de servidores de aplicaciones autorizados, así como políticas de privacidad para los usuarios.

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 (PS) y conmutación de circuitos (CS), la HSS contiene funcionalidades de Home Location Register (HLR) y Authentication Center (AUC), tal y como define el 3GPP.

El modelo del 3GPP diferencia entre dos dominios principales: el dominio CS (Circuit Switched) son aquellas redes basadas en conmutación de circuitos, tales como las redes RTC/RDSI o las redes de telefonía móvil 2G. El otro dominio es el PS (Packet Switched), el cual está formado por el propio núcleo IMS y el EPS (Evolved Packet System). Ambos dominios están interconectados a través de pasarelas como la Media Gateway Control Function (MGCF).

Ved también

Tanto el Evolved Packet System como la Media Gateway Control Function (MGCF) han sido descritos anteriormente.

La funcionalidad de HLR se requiere para dar soporte a entidades del dominio de PS, como el SGSN y el GGSN, permitiendo que el subscriptor se conecte a los servicios de la red de conmutación de paquetes. Del mismo modo, la HLR también posibilita el soporte a entidades de conmutación de circuitos, como los servidores MSC/MSC, que permiten el acceso del subscriptor a servicios del dominio CS y el *roaming* a redes GSM y UMTS.

Por su parte, el AUC almacena una clave secreta para cada subscriptor móvil, que se usa para generar datos dinámicos de seguridad. Estos datos son utilizados para la autenticación mutua del IMSI (International Mobile Subscriber Identity) y la red, así como para encriptar la comunicación radio entre el UE y la red.

Diferencias a destacar para modelo de la ETSI-TISPAN con respecto al 3GPP

- La entidad HSS pasa a llamarse User Profile Subscription Function (UPSF).

- La UPSF se puede considerar como un subconjunto de la HSS que excluye las funcionalidades de HLR y AUC, y que almacena únicamente datos relacionados con IMS.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- La entidad Service User Profile Functional Entity (SUP-FE) se corresponde con la parte del UPSF de TISPAN que gestiona los perfiles de usuario.

- La entidad Service Autentication & Autorization Functional Entity (SAA-FE) se corresponde con la parte del UPSF de TISPAN que gestiona la autorización y la autenticación.

Función de Localización de Suscripción (SLF)

Cuando existe más de una HSS en la red, es precisa la implementación de una entidad SLF y de sus puntos de referencia llamados Dx (conexión con las entidades de control de sesión de llamada: CSCF) y Dh (conexión con servidores de aplicaciones: AS).

En una red en la que se han desplegado múltiples HSS independientes, ni el I-CSCF ni el SCSCF conocen en cuál de estas HSS se encuentra la información que necesitan consultar. Por lo tanto, deben contactar en primer lugar con el SLF.

El SLF debe proveer de una funcionalidad de encaminado que permita que otras entidades descubran qué nodo HSS contiene la información de suscripción de un determinado usuario (identidad pública o MSISDN), otorgando al operador la flexibilidad de distribuir sus usuarios libremente entre varias HSSs.

Diferencias a destacar para el modelo de la ETSI-TISPAN con respecto al 3GPP

- No hay diferencias.

Diferencias a destacar para el modelo de la ITU-T con respecto al 3GPP

- Nombre de esta entidad cambia a Subscription Locator Functional Entity (SL-FE).

1.3.3. Otros componentes del modelo de la ETSI-TISPAN de control de servicio

La ETSI-TISPAN (ver la figura 14) incorpora una entidad funcional que no aparece en otras arquitecturas de control de servicio.

Función de Interoperabilidad (IWF): La Interworking Function se considera una entidad externa al núcleo IMS en sí. Se comunica con el núcleo vía una interfaz llamada Ib para garantizar la interacción entre protocolos empleados en los subsistemas de control de servicios NGN (SIP-IMS) y otros protocolos IP. Esta traducción de protocolos IP de señalización se plasma sobre una interfaz llamada Iw, que le interconecta con el dominio externo que soporta otros protocolos.

Por ejemplo, puede traducir entre los perfiles SIP de IMS y otros perfiles SIP, u otros protocolos basados en IP como H.323.

Diferencias a destacar para el modelo de la ITU-T con respecto al ETSI-TISPAN

- Las funciones que realiza el IWF se pueden mapear a la entidad equivalente en el modelo de la ITU-T: el Network Signalling Interworking Functional Entity (NSIW-FE). El NSIW-FE también tiene como tarea traducir a protocolos de señalización de redes de circuitos y en este caso se mapearía a MGCF.

1.3.4. Otros componentes del modelo de la ITU-T de control de servicio

La ITU-T (ver la figura 13) incorpora tres entidades funcionales que no aparecen en otras arquitecturas de control de servicio.

- **Interacción de Señalización de Usuario (USIW-FE):** El User Signalling Interforking Functional Entity agrupa las funciones de interoperabilidad de redes y monitorización de información para diferentes tipos de señalización de aplicaciones (diferentes a SIP de IMS), en el lado del suscriptor. Puede estar situado al borde de la red de acceso o del núcleo de red para gestionar la señalización en el lado del suscriptor.

- **Control de Pasarela de Acceso (AGC-FE):** El Access Gateway Control Functional Entity controla uno o más AMG-FEs vía la interfaz S-T2 para acceder a los usuarios de redes básicas RTC/RDSI, gestionando el registro, la

autenticación y la seguridad de los mismos. Puede iniciar y terminar señalización de control de sesiones, flujos de control de sesión de *gateways* para controlar los AMG-FEs, o flujos de control UNI para proporcionar servicios complementarios de RDSI. Por otra parte, también puede reenviar flujos de control al S-CSC-FE, y procesar y reenviar peticiones del AMG-FE al S-CSC-FE, o al AS-FE pasando a través del S-CSC-FE.

- **Control de Servicios Generales (GSC-FE):** El General Services Control Functional Entity pretende proporcionar una plataforma que dé soporte a los futuros servicios que se planteen sobre redes de paquetes. El GSC-FE ha de actuar como un punto de contacto para las entidades funcionales de soporte de servicio y aplicaciones, así como para los terminales de usuario. Deberá autenticar las comunicaciones que se den entre ellos, y proporcionar información sobre los flujos de sesión y sus requisitos de QoS al PD-FE o al IBC-FE.

General Service Control-FE

El GSC-FE o General Service Control-FE es una entidad funcional creada por el ITU-T para copar aquellos servicios para cuya invocación no lleve asociada un establecimiento de sesión previa, como sí lo hace IMS. Es un esfuerzo que realiza la ITU-T con tal de incluir cualquier otro mecanismo de invocación de servicio futuro.

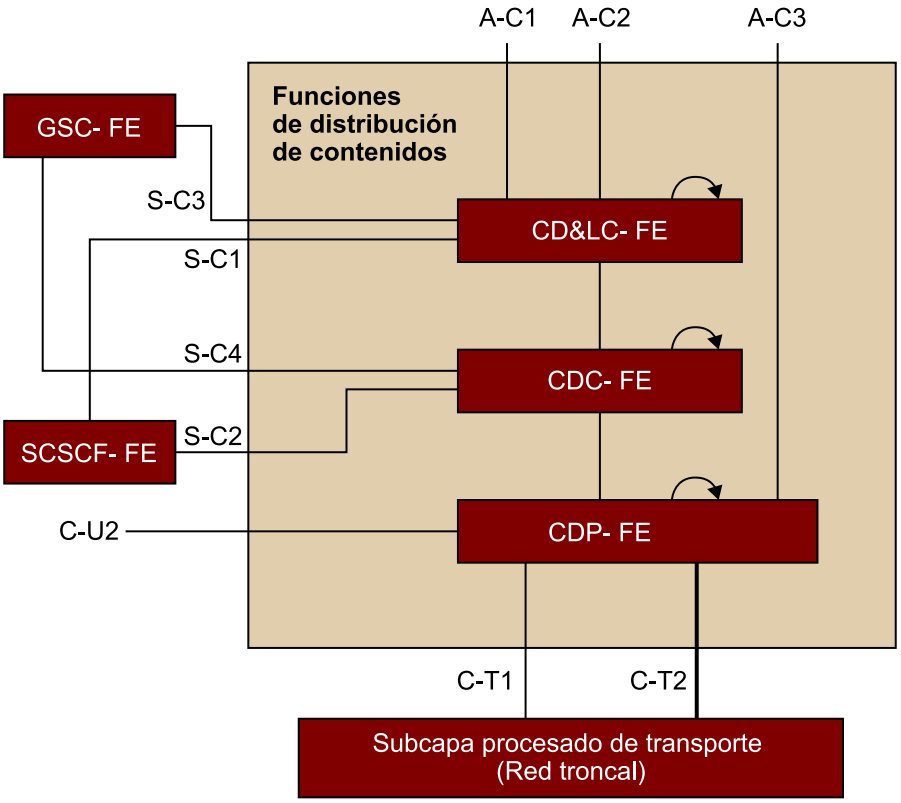
1.3.5. Componentes de la subcapa de distribución de contenido

Los componentes de las Content Delivery Functions (CDF) reciben contenidos desde la subcapa de las funciones de Soporte a Aplicaciones y Soporte a Servicios (ASF&SSF), los almacena, los procesa y los entrega a las funciones de usuario utilizando las capacidades de la funciones de transporte bajo control de la subcapa de control de servicio.

Estos componentes los ha definido la ITU-T para permitir a los servicios de IPTV, entre otros, distribuir sus contenidos entre los usuarios, tanto si son *unicast* como si son *multicast*.

No obstante, la ITU-T no cierra la puerta a que opcionalmente estos servicios de distribución sean llevados a cabo fuera del ámbito de las redes NGN.

Figura 16. Arquitectura de las funciones de distribución de contenidos



Si echamos un vistazo a la figura 16, vemos las entidades funcionales y las interfaces que los interconectan. Los puntos de referencia S-C1 y S-C2 corresponden al servicio de IPTV basado en IMS, mientras que los puntos de referencia S-C3 y S-C4 son para el servicio de IPTV no basado en IMS.

Control de Entrega y Control de Localización (CD&LC-FE)

El Delivery Control and Location Control Functional Entity (CD&LC-FE) realiza las siguientes funciones:

- Interacción con las entidades funcionales de control de servicio.
- Control de la distribución del contenido desde el CPR-FE (Preparación de Contenido) en la subcapa de soporte a servicios y aplicaciones hacia el CDP-FE.
- Aglutinamiento de la información acerca de las CDP-FE (uso de recursos, si está o no en servicio o estado de carga).
- Selección del o los CDP-FE para servir a las funciones de usuario en función de la información aglutinada y las capacidades del terminal de usuario.

Control de Distribución de Contenidos (CDC-FE)

El Content Delivery Control Functional Entity (CDC-FE) gestiona las funciones de control relacionadas con el CDP-FE. Parte de las funciones que realiza el CDC-FE son:

- Control de la entrega de recursos de medios.
- Gestión de los comandos de recodificación tales como para los VCR (Video Cassette Recorder).
- Reporte de información de estado (nivel de carga y disponibilidad) al CD&LC-FE.
- Generación de información para facturación.

Procesado de Distribución de Contenidos (CDP-FE)

El Content Delivery Processing Functional Entity (CDP-FE) almacena y guarda el contenido, lo procesa bajo control del CPR-FE (en la subcapa de soporte a servicios y aplicaciones) y el CDC-FE. El CDP-FE distribuye el contenido entre instancias de CDP-FE basadas en la política del CD&LC-FE.

El CDP-FE es responsable de entregar el contenido a las funciones de usuario usando las funciones de transporte (incluyendo mecanismo de unicast y multicast).

Otras funciones del CDP-FE:

- Interacción con las entidades funcionales de control de servicio.
- Gestión de la entrega de contenidos al usuario final.
- Almacenado del contenido e información asociada.
- Inserción, transcodificación y cifrado del contenido.
- Distribución de contenidos entre CDP-FE.
- Gestión de la interacción con el usuario final: funciones de control de visualización del contenido (en el caso de vídeo) como por ejemplo, rebobinar, ir hacia delante, pausa, etc.

1.3.6. Subcapa de Soporte a Servicios y Soporte a Aplicaciones

La ITU-T concentra las funciones relacionadas estrictamente con la provisión de servicios en una subcapa dentro de la capa de servicio (ver la figura 1) llamada **subcapa de soporte a aplicaciones y soporte a servicios** (ASF&SSF), que complementan a los bloques de la subcapa de control de servicio, donde se ubicaría el núcleo IMS (ver la figura 13).

El módulo de ASF&SSF controla los servicios ofrecidos mediante la interacción con la S-CSC-FE (función equivalente al S-CSCF del 3GPP) vía una interfaz llamada A-S4 (equivalente al ISC del 3GPP), la GSC-FE vía una interfaz llamada A-S2 o el usuario final vía una interfaz llamada A-U1. Puede estar situado tanto en la red local de usuario como en una tercera red, y comprende las siguientes entidades funcionales: Servidor de Aplicaciones (Application Server FE), Gateway de Aplicaciones (Application GW FE), Gestión de Coordinación entre Servicios de Aplicaciones (Application Service Coordination Manager FE) y Entidad Funcional de Conmutación de Servicios (Service Switching FE).

Este módulo genera las peticiones de control de sesión y los diálogos en representación del usuario. Asimismo, ejecuta la lógica de servicio basada en los perfiles de usuario y de terminal (capacidades del dispositivo).

El módulo ASF&SSF puede actuar de acuerdo a cuatro modelos de interacción de sesión con relación al S-CSC-FE: agente de usuario de terminación, agente de usuario de origen, proxy SIP o controlador de llamada *third-party*.

En lo referente a su interacción con las entidades del plano de control de servicio, el ASF&SSF puede interactuar con el AGC-FE (Access Gateway Control Functional Entity) a través del S-CSC-FE para permitir el acceso a las aplicaciones a aquellos usuarios que emplean terminales tradicionales RTC o RDSI. Puede también controlar recursos multimedia (tonos, mensajes audio de espera, etc.) con el MRP-FE (Media Resource Processing Functional Entity) a través del MRC-FE (Media Resource Control Functional Entity) vía la interfaz A-S3 o el S-CSC-FE vía la interfaz A-S4. Puede finalmente acceder al MRB-FE (Media Resource Broker Functional Entity) vía la interfaz A-S1 para asignar recursos multimedia a las llamadas o relacionarse con las funciones de usuarios finales para permitir que estos gestionen y configuren sus datos para los servicios de aplicaciones.

2. 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 en la red troncal de transporte: modo *push* o modo *pull*.

Estos dos mecanismos intentan adaptarse a cualquier red de acceso que pueda existir en términos de reserva de recursos y negociación de QoS en la capa de transporte. Es decir, habrá redes de acceso que posean estos mecanismos en capa 2 ya definidos y habrá redes que no los posean. En este sentido, se pueden clasificar los equipos de usuario en tres tipos. Esta clasificación nos servirá para saber qué tipo de mecanismo (*push* o *pull*) se puede relacionar a cada tipo de terminal:

- **Tipo 1.** Equipo de usuario sin capacidad de negociación de QoS ni en la capa de servicio ni en la de transporte. Puede comunicarse con el núcleo IMS (o entidad equivalente de la capa de servicio) para iniciar y negociar el servicio, pero no puede solicitar recursos directamente.

  Un ejemplo del tipo 1 sería una consola de juegos.

- **Tipo 2.** Equipo de usuario con capacidad de negociación de QoS a nivel de capa de servicio. Usando la señalización IMS negocia la QoS, como el ancho de banda requerido, pero desconoce totalmente los parámetros de QoS equivalentes aplicables a la red de transporte.

  IMS negocia la QoS usando SDP (Session Description Protocol, RFC 4566) integrado dentro de los mensajes SIP.

- **Tipo 3.** Equipo de usuario con capacidad de negociación de QoS a nivel de capa de transporte (tipo protocolo RSVP u otro protocolo de transporte). Es capaz de realizar directamente negociación de QoS de transporte a lo largo de toda la infraestructura de transporte (por ejemplo, DSLAM para ADSL, CMTS para cable, SGSN/GGSN para telefonía móvil).

  Ejemplos del tipo 3 sería un terminal LTE.

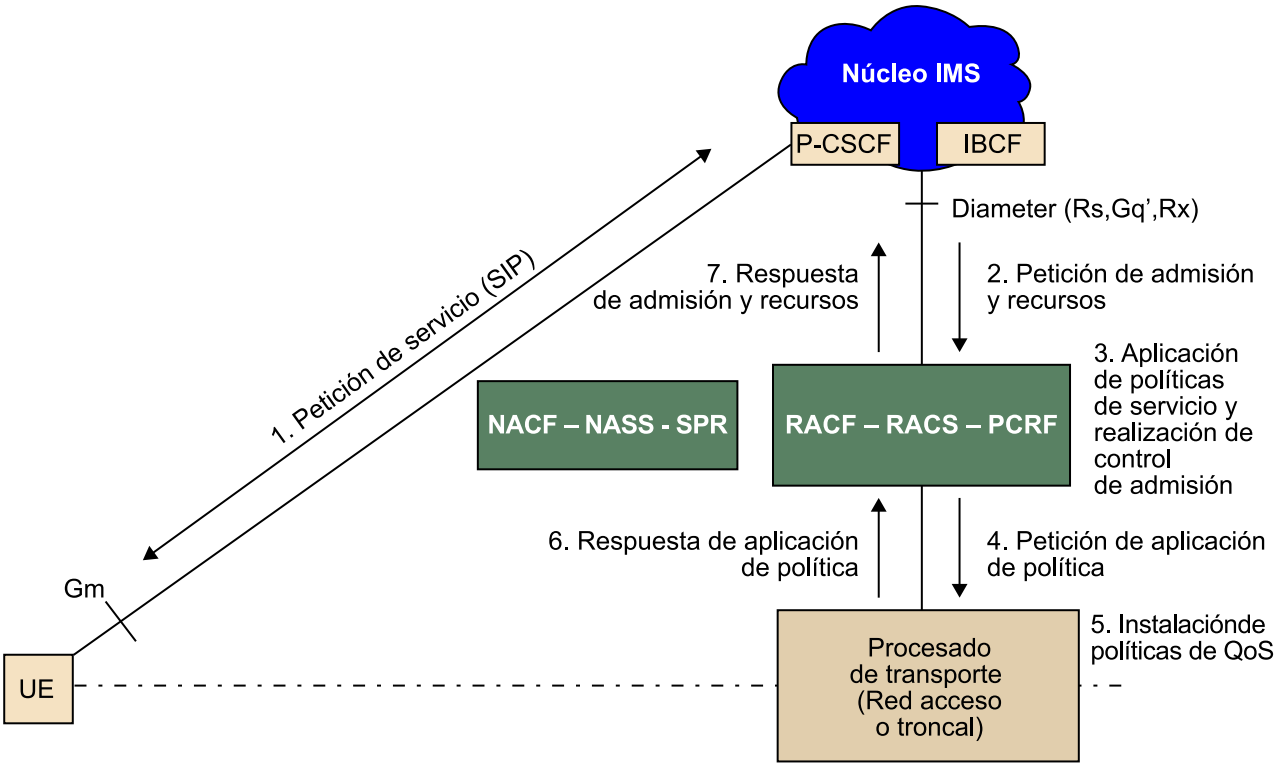
2.1. Modo *push*

La figura 17 nos muestra paso a paso el proceso de reserva de recursos y garantía de QoS correspondiente al modo *push*. Fijaos 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 el IBCF si es la red troncal) y posteriormente se traduce en la instalación de políticas de QoS sobre la capa de procesado de transporte.

En este caso, los tipos de terminales que se adaptan a este mecanismo en modo *push* son aquellos que no tienen capacidad de negociar la QoS directamente en la capa de transporte: tipo 1 y tipo 2.

Figura 17. Mecanismo de reserva de recursos en modo *push*



Veamos con un poco más de detalle qué sucede en cada paso:

1) El equipo de usuario (UE) inicia la petición de servicio enviando un SIP INVITE. Si el UE es de tipo 1, envía el mensaje SIP con sus cabeceras pertinentes, pero si es de tipo 2 incluye una cabecera extra de SDP con la especificación de QoS a nivel de aplicación o servicio que solicita, en el que incluye la solicitud de recursos. El P-CSCF reenvía dicho mensaje al S-CSCF y espera un mensaje de respuesta que contenga la réplica al INVITE con la propuesta final de QoS negociada en la cabecera SDP. De ahí el P-CSCF extrae los parámetros de QoS que necesita para realizar la solicitud de reserva de recursos a la entidad que realiza el control de admisión de recursos en la red de acceso. Si el terminal es de tipo 1, no habrá SDP, pero igualmente el P-CSCF debe extraer parámetros de QoS basándose en políticas propias prefijadas.

2) El P-CSCF, vía la interfaz Diameter correspondiente, solicita la autorización QoS y la reserva de recursos con los parámetros QoS explícitos hacia la entidad que controla los recursos en la red de acceso (subcapa de control de transporte). Dicha solicitud se lleva a cabo con un mensaje AAR (AA-Request), el cual incluye una descripción detallada de los componentes multimedia de la solicitud (información de ancho de banda, tipo de datos y otros parámetros de QoS por cada flujo IP que los componen).

Lectura complementaria

Para conocer los parámetros de los mensajes Diameter de la interfaz Rx, leed el documento 3GPP TS 29.214. Para el caso de la interfaz Gq' recurrid al ETSI TS 183 017.

3) La entidad de control de transporte recibe la petición y aplica las políticas de red a dicha solicitud (reglas arbitrarias de operador) para poder autorizarla. Luego aplica el control de admisión consultando primero el perfil de usuario y luego la disponibilidad de los recursos solicitados en el sistema. Si todos los controles son superados y esta entidad decide que es necesario instalar las políticas de QoS pertinentes (también hay que tener en cuenta si desde el P-CSCF se ha solicitado en una sola fase la asignación final de recursos o *Commit*), se generan dichas políticas de QoS a partir de la solicitud recibida desde el P-CSCF para ser instaladas en las entidades de procesado de transporte pertinentes.

4) Las entidades reciben las políticas de QoS a instalar, cuya especificación puede ser tan simple como el nombre de una política ya predefinida o también una descripción detallada de dicha política (ya sea con parámetros de QoS dependientes de la tecnología o no). En Diameter, para instalar estas políticas de QoS, se utilizan mensajes como PIR (Policy Installation Request) en el caso de la interfaz Re de la ETSI-TISPAN o RAR (Re-Auth Request) en el caso de la interfaz Gx del 3GPP.

5) Las políticas se instalan convirtiendo aquellos parámetros de QoS que sean independientes de la tecnología en parámetros instalables y adaptados a parámetros de la propia tecnología. Aquí se lleva a cabo también la asignación de recursos al UE de acuerdo con la definición de tales políticas de QoS.

6) La entidad que se encarga de la aplicación de las políticas de QoS notifica al gestor de recursos de la red de acceso del éxito de dicha instalación. Para ello, en Diameter se usa los respectivos mensajes de respuestas PIA (Policy Installation Answer) o RAA (Re-Auth Answer) según sea ETSI-TISPAN o 3GPP respectivamente.

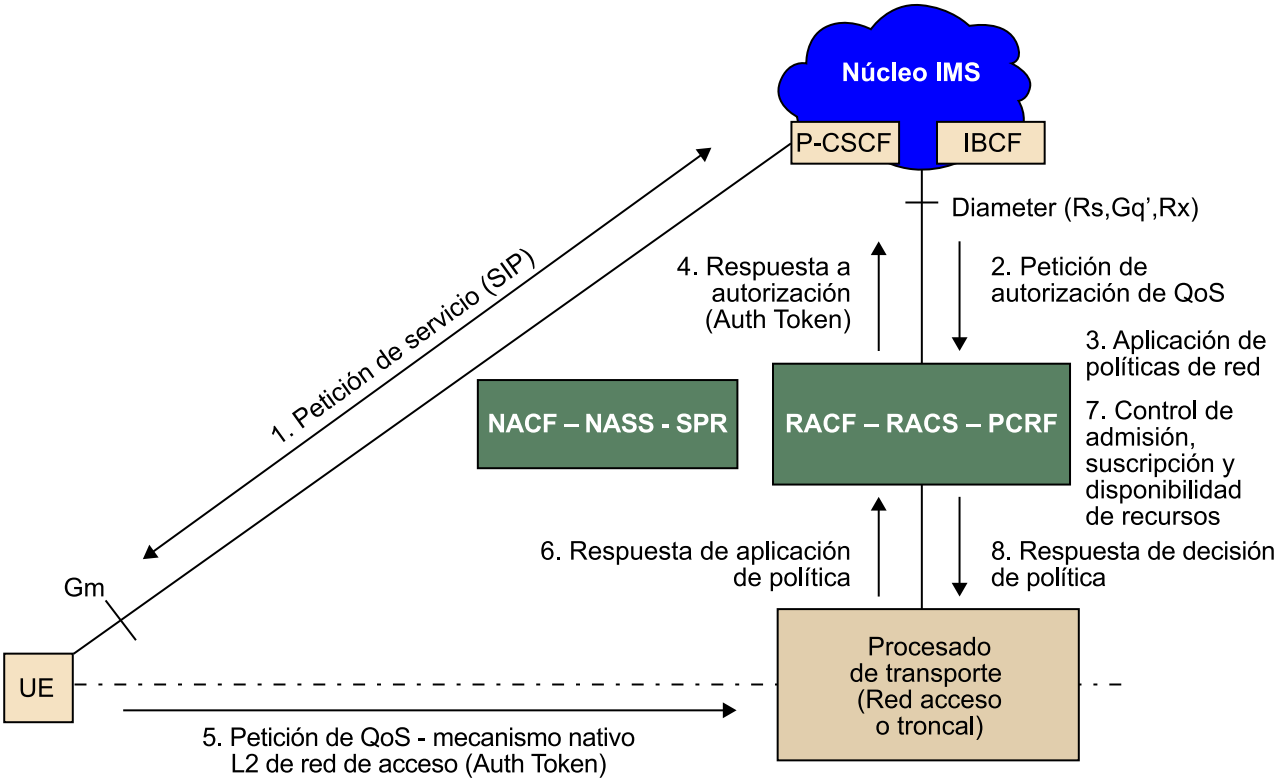
7) La entidad de control de transporte espera las respuestas de todas las entidades a las que ha solicitado la instalación de políticas antes de enviar una respuesta con la decisión final sobre la solicitud de recursos al P-CSCF. En Diameter, se utiliza el mensaje AAA (AA Answer).

2.2. Modo *pull*

La figura 18 nos muestra paso a paso el proceso de reserva de recursos y garantía de QoS correspondiente al modo *pull*. La reserva se divide en dos partes, una realizada desde el núcleo IMS para autorizar los recursos, y otra para asignar los recursos utilizando el mecanismo nativo de la red de acceso.

En este caso el único tipo de terminal que se adapta a este mecanismo en modo *pull* es el de tipo 3.

Figura 18. Mecanismo de reserva de recursos en modo *pull*



Veamos con un poco más de detalle qué sucede en cada paso:

1) El equipo de usuario (UE) inicia la petición de servicio enviando un SIP INVITE. El UE incluye una cabecera extra de SDP con la especificación de QoS a nivel de aplicación o servicio que solicita en el que incluye la solicitud de recursos. El P-CSCF reenvía dicho mensaje al S-CSCF y espera un mensaje de respuesta que contenga la réplica al INVITE con la propuesta final de QoS negociada en la cabecera SDP. De ahí el P-CSCF extrae los parámetros de QoS que necesita para realizar la solicitud de reserva de recursos a la entidad de realizar el control de admisión de recursos en la red de acceso.

2) El P-CSCF, vía la interfaz Diameter correspondiente, solicita el control de admisión y la reserva recursos con los parámetros QoS extraídos a la entidad que controla los recursos en la red de acceso (subcapa de control de transporte). Para ellos se usa el mensaje AAR ya mencionado.

3) La entidad de control de transporte recibe la petición de autorización de QoS y aplica las políticas de red a dicha solicitud (reglas arbitrarias de operador). Si la petición es autorizada puede crear opcionalmente un *token* de autorización con un único identificador que representa a la petición de QoS.

4) El bloque de control de recursos responde a la petición (mensaje Diameter AAA) y si ha sido satisfactoria puede incluir el *token* creado para que el P-CSCF lo incluya en el mensaje SIP de vuelta al UE.

5) El UE solicita directamente a las entidades de transporte los recursos para albergar el tráfico del servicio solicitado. Puede opcionalmente incluir información de QoS así como el *token* de autorización para ayudar a la entidad de control de transporte asociar la solicitud de recursos con la solicitud autorizada en los pasos previos. La asociación se puede realizar con otros métodos.

6) Las entidades de procesado de transporte detectan la petición de recursos remitida por el UE y transfieren dicha petición en forma de petición de decisión de política a la entidad de control de transporte. Si el *token* ha sido incluido en la solicitud de recursos, éste puede ser traspasado también. En este caso, tanto para el caso de la interfaz Re de la ETSI TISPAN como de la interfaz Gx del 3GPP se utiliza el mensaje CCR (Credit Control Request), pero el formato interno ligeramente puede variar en función de la especificación.

Lectura complementaria

Para conocer los parámetros de los mensajes Diameter de la interfaz Gx, recurrid al documento 3GPP TS 29.212. Para el caso de la interfaz Re recurrid al ETSI TS 183 060.

7) La entidad de control de transporte aplica entonces el control de admisión para los recursos solicitados consultando primero el perfil de usuario y luego la disponibilidad de los recursos solicitados en el sistema. Si la solicitud de recursos implica hacer reserva y asignación en una sola fase, elabora las políticas de QoS a instalar en las entidades de procesado de transporte que éste crea oportuno (inclusive la asignación de los recursos).

8) Las entidades de procesado de transporte reciben la respuesta del control de admisión (mensaje CCA) y aplican las políticas de QoS derivadas de tal decisión para asignar los recursos solicitados por el UE.

Los pasos del 1 al 4 en los que se realiza una autorización mediante el *token* son opcionales, ya que la asociación entre la solicitud autorizada y la petición de recursos desde la subcapa de procesado de transporte puede realizarse de otras maneras.

3. 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 y H.248. En este apartado veremos las principales características de cada uno pero focalizándonos más en los dos primeros ya que tienen muchas más presencia y complejidad.

3.1. 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.

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 alcanzable vía una dirección, por medio de una SIP URI.

Es importante resaltar que SIP es un protocolo de señalización para iniciar, modificar y liberar sesiones multimedia. Por otra parte, SIP no es un protocolo de reserva de recursos y, en consecuencia, no puede asegurar la calidad de servicio. Se trata de un protocolo de control de llamada y no de control del medio. 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). El protocolo SIP puede usarse bajo TCP, UDP o SCTP.

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.

3.1.1. 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.

- **Servidor de Redirección** (Redirect Server): se trata de un servidor quien acepta solicitudes SIP, traduce la dirección SIP de destino en una o varias direcciones 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 numero de reenvió de llamada y encaminar la llamada a este nuevo destino, y eso de manera transparente para el cliente de origen; para el mismo servicio, el Redirect Server devuelve el nuevo número (número de reenvio) 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. Se materializa por un software instalado sobre un UE.

- **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.

3.1.2. 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 cabecear 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@213.20.128.35
CSeq: 2 INVITE
Contact: <sip:213.20.128.35:9315>
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 213.20.128.35
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 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 dialogo 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 enviados por el usuario llamado.

Las otras 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.

Mètodos SIP

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

Tabla 1. Métodos SIP

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.

Método	Descripción
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 hacia un tercer UA. Permite emular distintos servicios o aplicaciones incluyendo la transferencia de llamada (RFC 3515).
MESSAGE	Transporta mensajes instantáneos de texto usando SIP. El requerimiento 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 dialogo SIP. Permite a un terminal SIP actualizar los parámetros de una sesión multimedia (flujo media y sus códecs). El método UPDATE puede ser enviado antes de que la sesión sea establecida (RFC 3311).

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 2. Códigos de respuestas SIP

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

3.1.3. 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[3]: 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.

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.

[3]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*.

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 suplementales 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.

3.2. 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 (RFC 3588). 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.

3.2.1. Nodos y agentes Diameter

El protocol Diameter está diseñado para arquitecturas *peer-to-peer*. Cada *host* que implementa el protocol 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 envia 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).

3.2.2. 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.

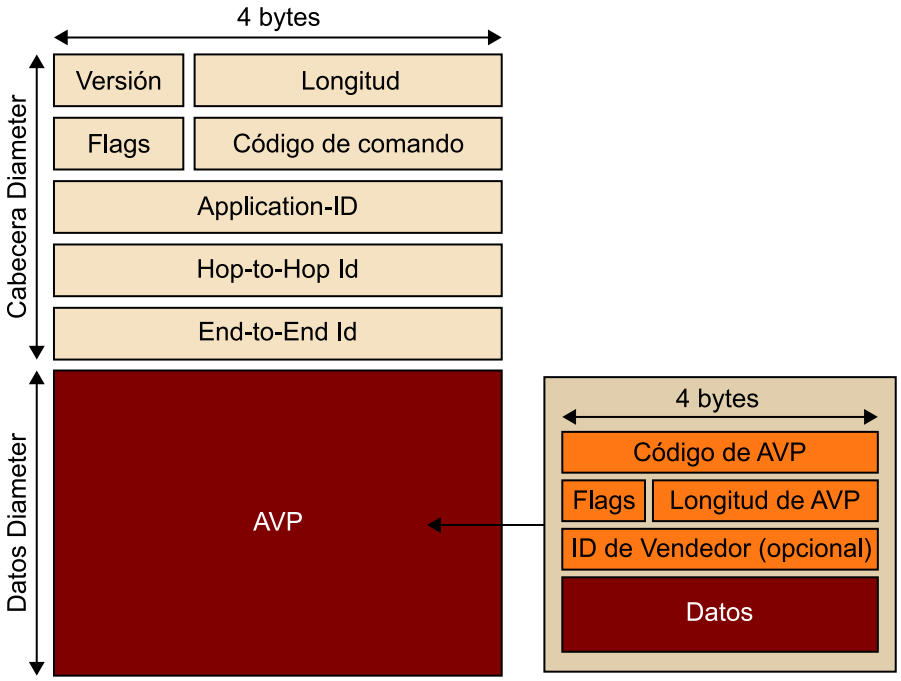
Como el intercambio de mensajes en Diameter es síncrono, cada mensaje tiene su contraparte correspondiente (petición-respuesta), que comparte el mismo código de comando.

> 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 antes que nada 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 definidos en el Diameter Base Protocol (por ejemplo, OctetString, Integer32), con lo que cada AVP debe seguir el formato de datos concreto. La figura 19 muestra los campos que componen un mensaje de Diameter.

Figura 19. Campos de mensaje Diaemter 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[4]).

(4)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.

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).

Según la especificación de la aplicación de Diameter a implementar, se pondrá un valor en el campo de Application-ID[5] u otro (asignado también por la IANA).

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

Entidades de estandarización como 3GPP y ETSI-TISPAN

Las entidades de estandarización, como el 3GPP y la ETSI-TISPAN, 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. Tened en cuenta que hay definiciones de AVP que se comparten entre especificaciones entre dos interfaces porque hacen la misma función o incluso se comparten entre especificaciones de distintas entidades de estandarización. Puede que haya AVP con vendor ID 3GPP usados en especificaciones de la ETSI-TISPAN y viceversa. Esto es resultado de uniformizar las distintas implementaciones.

3.3. Protocolo H.248 / MEGACO

El H.248 es un protocolo definido por la ITU-T, aunque hay una implementación equivalente del IETF llamado MEGACO (RFC 3525). Es un protocolo para controlar los elementos de una pasarela multimedia físicamente separada, que habilita la separación del control de llamada de la conversión de medios.

Es un protocolo basado en una arquitectura maestro/esclavo usado para separar la lógica del control de llamada del procesado de los medios.

En IMS se utiliza para controlar pasarelas localizadas en la subcapa de procesado de transporte e instalar configuraciones de apertura de control de acceso a modo de cortafuegos y fijar traducciones.

4. Ejemplos de flujos de llamadas en NGN 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 dos ejemplos que vamos a ver son el proceso de registro en IMS en el que se muestran las dos fases:

1) Adhesión a la red según el modelo de la ETSI-TISPAN y luego el 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.

También se incluye al final un ejemplo del servicio de presencia en IMS, como muestra de la interacción con un servidor de aplicaciones (AS).

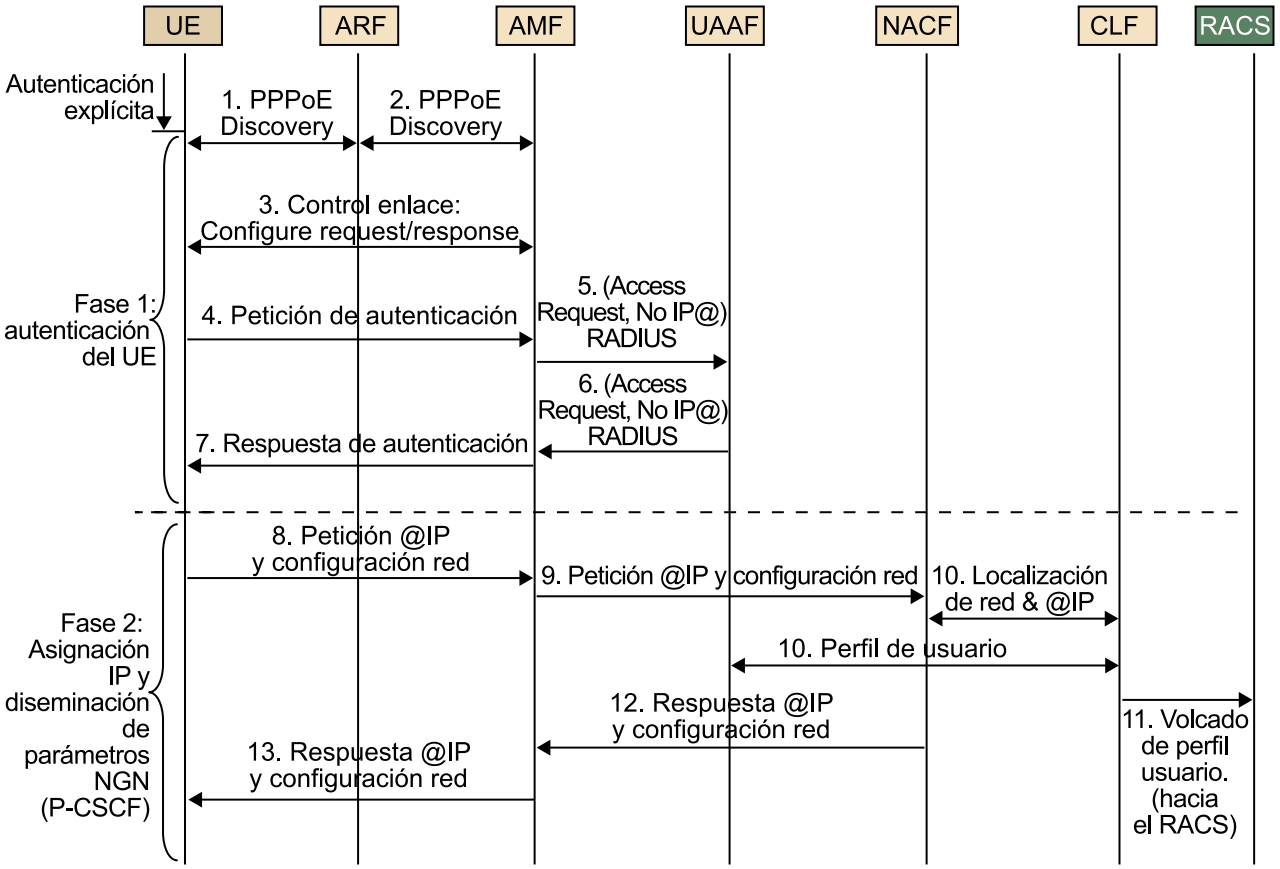
4.1. Adhesión a la red

Seguidamente vamos a ver mensaje a mensaje el proceso de adhesión de un UE a la red de acceso y cómo posteriormente se registra en el núcleo IMS.

4.1.1. Fase de autenticación del equipo de usuario y asignación de IP

La siguiente figura muestra paso a paso un ejemplo de adhesión a la red con autenticación explícita por parte de un router ADSL (UE) al registrarse en la red de acceso usando PPPoE como protocolo de establecimiento de conexión en capa 2.

Figura 20. Paso a paso de adhesión de un UE a la red de acceso (ejemplo basado en especificación de ETSI-TISPAN)



a) Pasos 1 y 2: el UE realiza los procedimientos de PPPoE discovery para identificar el AMF apropiado y establece una relación *peer-to-peer* con el AMF, tal y como se requiere en PPP. El ARF implementa un agente intermedio de PPPoE e inserta la identificación de línea de acceso en los mensajes de PPPoE.

b) Paso 3: Inicia la fase LCP (Link Control Protocol) del PPP. Negociación de parámetros de enlace de datos entre el UE y el AMF incluyendo la negociación del procedimiento de autenticación a usarse.

c) Paso 4: el UE inicia la autenticación y envía la correspondiente información (identidad del usuario e información sobre la contraseña) al AMF.

d) Paso 5: el AMF traduce la petición PPP al mensaje equivalente de RADIUS (AMF hace de cliente) para solicitar acceso al UAAF que autentica la identidad del usuario asociado al UE.

e) Paso 6: el UAAF contesta al AMF reportando autenticación exitosa.

f) Paso 7: el AMF envía el mensaje PPP correspondiente para reportar dicha autenticación exitosa. Finaliza la fase LCP del PPP. El usuario ha sido autenticado en la red de acceso con éxito.

Nota

En el caso hipotético de un escenario de itinerancia, el UAAF de la red visitada actuaría como UAAF proxy (proxy RADIUS en este ejemplo) y reenviaría la petición de autenticación por la interfaz e5 al UAAF correcto.

g) Paso 8: inicia la fase de NCP (Network Configuration Protocol) del PPP. Solicita al AMF la asignación de una dirección IP.

h) Paso 9: el AMF traduce dicha solicitud de dirección IP a RADIUS y la envía al NACF.

i) Paso 10: el NACF selecciona una IP de su repositorio y vuelca esta información al CLF. Del mismo modo, el UAAF vuelca al CLF el perfil de usuario una vez ya está autenticado.

Nota

El UAAF puede volcar la información de perfil de usuario tan pronto como el UE se autentica con éxito. No hace falta que espere al NACF para que le asigne la dirección IP. El CLF es capaz de recibir ambas informaciones y asociarlas a posteriori.

j) Paso 11: tan pronto como el CLF recibe la información del NACF y del UAAF, vuelca la información integrada al RACS (vía la interfaz e4 basado en Diameter) para que lo tenga presente si dicho UE solicita en un futuro un servicio con requerimientos de QoS.

k) Paso 12 y 13: el NACF le proporciona (vía el AMF traduciéndolo a PPP) la dirección IP asignada e información sobre el P-CSCF (*hostname*) al cual se debe dirigir.

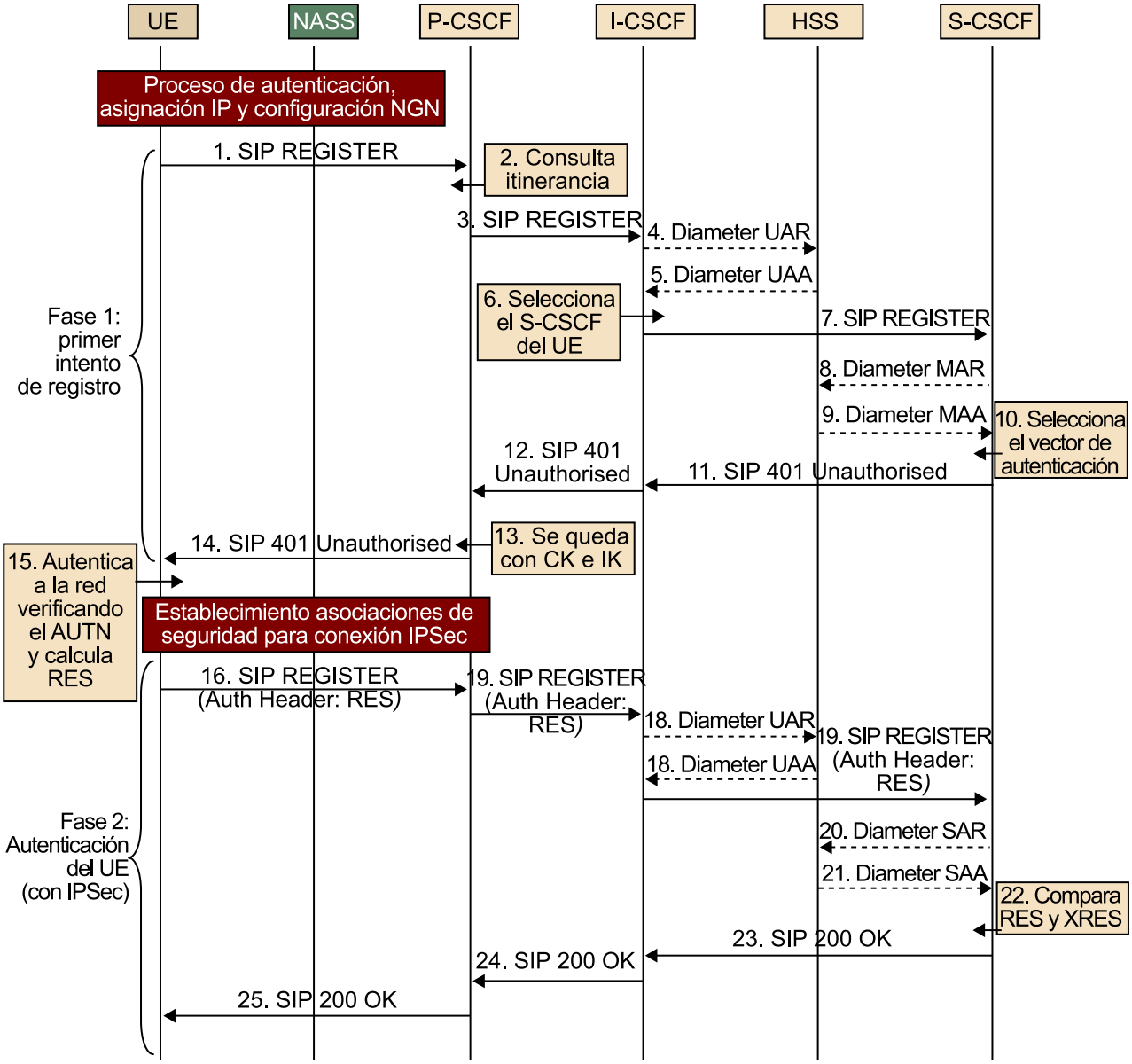
A partir de este instante, el UE ya dispone de una dirección IP, que es única en el ámbito de la red de acceso (ya sea pública o privada). Consecuentemente, el UE puede solicitar servicios IMS a través de la interfaz Gm una vez esté registrado en el núcleo IMS.

Cabe mencionar que los protocolos de autenticación y asignación de IP pueden variar. En lugar de PPP puede usarse 802.1x y DHCP para solicitud de IP y diseminación de configuración de núcleo IMS.

4.1.2. Fase de registro en el núcleo IMS

La siguiente figura muestra los pasos que da un UE para registrarse en el núcleo IMS. En este caso, no importa qué implementación se use para la red de acceso, ya que IMS es independiente de ésta.

Figura 21. Paso a paso de registro en núcleo IMS



a) Paso 1: el UE (cliente IMS) envía un mensaje SIP REGISTER hacia la IP del P-CSCF cuyo *hostname* ha recibido desde el NASS. La IP la descubre vía consulta de DNS. Añade una cabecera *Via:* con su *hostname* para notificar que el mensaje ha pasado por él.

b) Paso 2: el P-CSCF recibe el SIP REGISTER y gracias a la cabecera *Contact:* conoce la dirección IP asignado 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.

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

d) 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.

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

f) 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*.

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

h) 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.

i) 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).

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

k) 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.

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

m) Paso 13: aquí el P-CSCF extrae de la cabecera *www-Authenticate:* el CK y el 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.

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

ñ) 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).

o) 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 caberera *Authorization*.

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

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

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

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

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

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

v) 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).

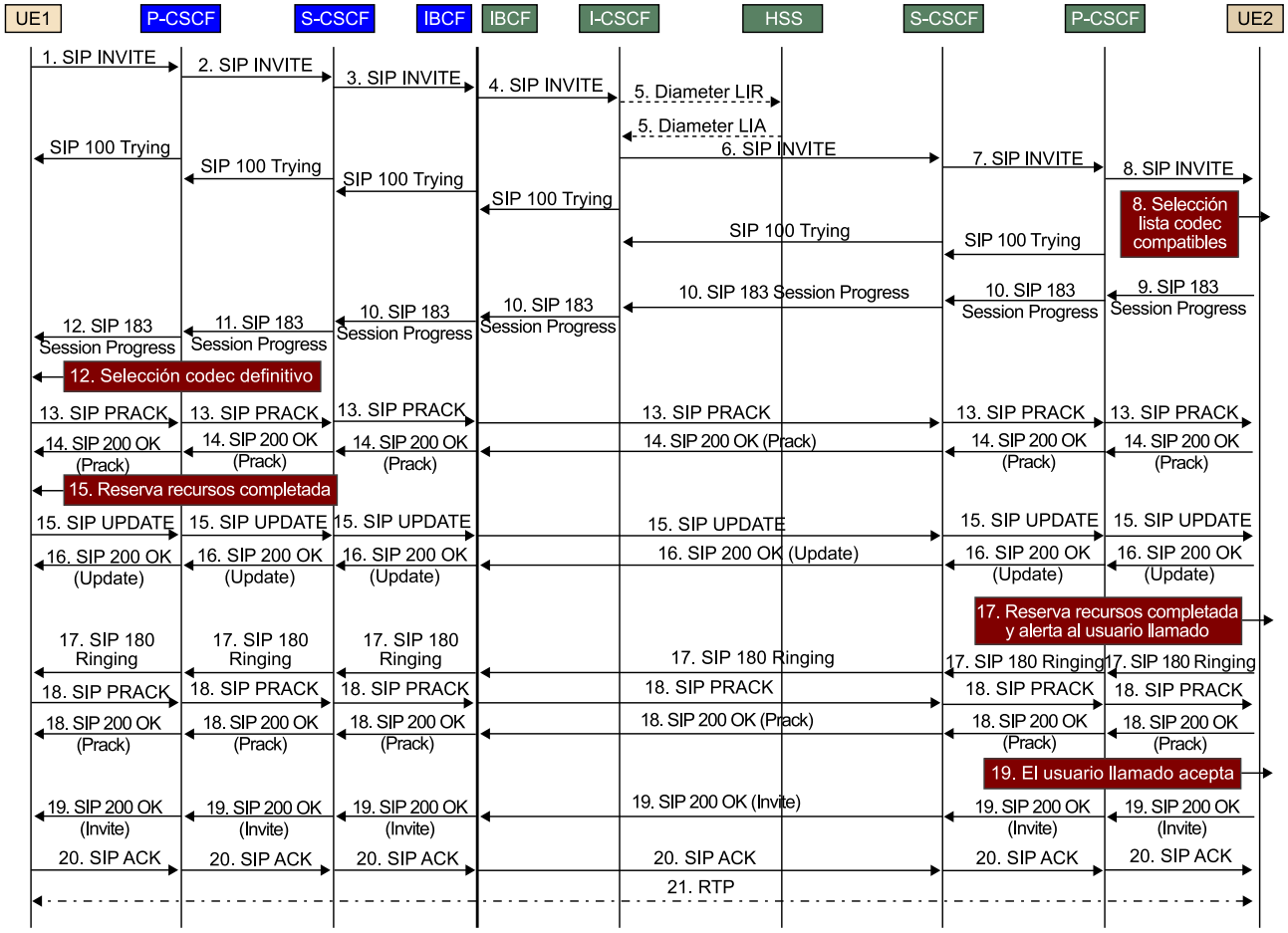
4.2. Establecimiento de sesiones de servicios

Seguidamente vamos a ver primero 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. A continuación, veremos cómo funciona el servicio de presencia en IMS.

4.2.1. Sesión IMS de servicio de voz

La siguiente figura 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 22. Flujo de llamada de voz en IMS



1) 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 la 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.

2) 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 muestra 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.

Nota

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 Triying. Esto se repite para todos los demás elementos que procesan la petición SIP INVITE en el camino.

c) 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*.

Nota

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.

d) 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*.

Nota

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 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).

e) 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.

f) 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*.

g) 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:

- Modo *pull:* el P-CSCF solicitaría al PCRF/RACS/RACF un *Authorization token* para incluirlo en el mensaje a enviar al UE 2.

- Modo *push:* el P-CSCF no solicita nada al PCRF/RACS/RACF porque solo tiene la información de QoS del UE. Reenvía el mensaje al UE 2.

Nota

Para el caso concreto del modo *push*, cabe la posibilidad que el P-CSCF esté configurado para que realice una reserva de recursos a la red de acceso, pero incluyendo información de QoS propuesta solo por el UE 1, esperando que en sucesivos intercambios de mensajes SIP se actualice la información de QoS definitiva y por lo tanto, actualice los recursos reservados en la red de acceso.

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*.

h) Paso 8: el UE 2 recibe el SIP INVITE con la propuesta de códec del UE 1. Entonces 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 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.

i) 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/RACS/RACF no reenvía el mensaje SIP).

j) 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.

Nota

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.

k) Paso 11: la respuesta 183 Session Progress, con una cabecera SDP con una lista de parámetros de QoS pre-negociados entre en UE 1 y UE 2, llega al P-CSCF del dominio azul, el cual puede actuar de dos formas dependiendo del modelo de reserva de recursos de la red de acceso:

- Modo *pull*: en el caso de que el UE 1 estuviese en una red de acceso con mecanismos de reserva de recursos en capa 2, el P-CSCF solicitaría al PCRF/RACS/RACF un *Authorization token* para incluirlo en la respuesta a enviar al UE 1.
- Modo *push*: el P-CSCF solicitaría al PCRF/RACS/RACF la autorización de QoS y reserva de recursos, utilizando la primera selección de códecs propuesta en el SDP (normalmente, si hay más de una opción de códecs, la primera especificada en la lista es la preferida por ambos UE). La red de acceso inicia dicha reserva de recursos para el 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.

l) 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. Seguidamente, y ahora que ya tiene el códec definitivo, dependiendo del modelo de reserva de recursos de la red de acceso del UE 1, éste actuará de una forma u otra:

- Modo *pull*: inicia los mecanismos propios que tenga la red de acceso para garantizar la QoS negociada (ancho de banda en ambos sentidos entre otros parámetros de QoS). En dicha petición de recursos debe incluir el *Authorization Token*, si existe. En el mensaje PRACK a enviar con los códecs definitivos, se notifica al UE 2 el estado de la reserva de recursos con el atributo *a=curr: qos local none*. Con esto le indica que los recursos en la red local del UE 1 todavía no están disponibles (aunque realmente su reserva ya ha sido iniciada).

- Modo *push*: el UE 1 no debe realizar nada, ya que tan pronto como ha recibido el 183 Session Progress puede asumir que hay una reserva de recursos hecha (dependiendo de la tecnología de la red de acceso el UE 1 sería informado sobre los recursos asignados). En el mensaje PRACK a enviar con los códecs definitivos, el UE 1 ya estaría en posición denotificar al UE 2 con el atributo *a=curr: qos local sendrecv* de que una reserva de recursos ya ha sido realizada en su red de acceso.

Sobre el modo *push*

Referente al modo *push*, se puede encontrar software de clientes IMS que se ejecutan en PC conectados a una LAN, y por lo tanto, no reciben notificación alguna sobre la reserva de recursos. Pero no asumen ninguna reserva por el hecho de recibir el 183 Session Progress y no notificarían al UE 2 que hay una reserva de recursos en su red de acceso (incluyen el atributo atributo *a=curr: qos local none*), asumiendo que posteriormente habrá un intercambio de mensajes UPDATE /200 OK, donde sí se notificará sobre dicha reserva definitiva de recursos.

m) 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:

- Modo *pull*: inicia la reserva de recursos teniendo en cuenta el códec definitivo seleccionado. Contesta con un 200 OK (y el mismo contenido en la cabecera SDP) al PRACK notificando al UE 1 que la reserva de recursos aún no está disponible (*a=curr: qos local none*).
- Modo *push*: simplemente contesta con 200 OK notificando al UE 1 (con el mismo contenido en la cabecera SDP). El UE 2 puede asumir que al recibir el PRACK ya se ha realizado una primera reserva de recursos en su red de acceso (y estaría en posición denotificar al UE 2 con el atributo *a=curr: qos local sendrecv)*. Pero del mismo modo que en el paso 12 en modo *push*, el UE 2 podría esperar a recibir el mensaje UPDATE para notificar sobre el estado de su reserva de recursos.

n) 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*).

ñ) 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*. No obstante, dependiendo del modelo de reserva de recursos de la red de acceso, el mensaje UPDATE se enviará en un momento u otro:

- Modo *pull*: el UE 1 esperará a la reserva de recursos iniciada anteriormente (al recibir el PRACK y seleccionar el códec definitivo) para enviar el UPDATE con la actualización del estado de reserva en la cabecera SDP.
- Modo *push*: el UE 1 puede enviar el mensaje UPDATE directamente sin esperar, asumiendo que si ha llegado hasta este punto, todo ha ido bien en la reserva de recursos en su red de acceso.

o) 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. No obstante, dicho mensaje de respuesta llevará consigo la cabecera SDP con las condiciones negociadas de QoS:

- Modo *pull*: si el proceso de reserva de recursos iniciados al recibir el PRACK aún no ha finalizado, incluirá en la cabecera SDP el atributo *a=curr: qos local none*. Con esto da a entender al UE 1 que tan pronto como dichos recursos ya estén reservados en su red de acceso, enviará una respuesta 180 Ringing, para notificar que el teléfono del UE 2 está sonando (y por lo tanto, todos los recursos ya están reservados a lo largo de todo el camino).
- Modo *push*: el UE 2 puede asumir que llegado a este punto, el proceso de reserva de recursos ya ha sido completado y por lo tanto, envía el 200 OK y seguidamente el 180 Ringing.

El 200 OK en respuesta al UPDATE viaja hasta el UE 1 para notificarle la recepción de éste.

p) 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.

q) 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.

r) 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.

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

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

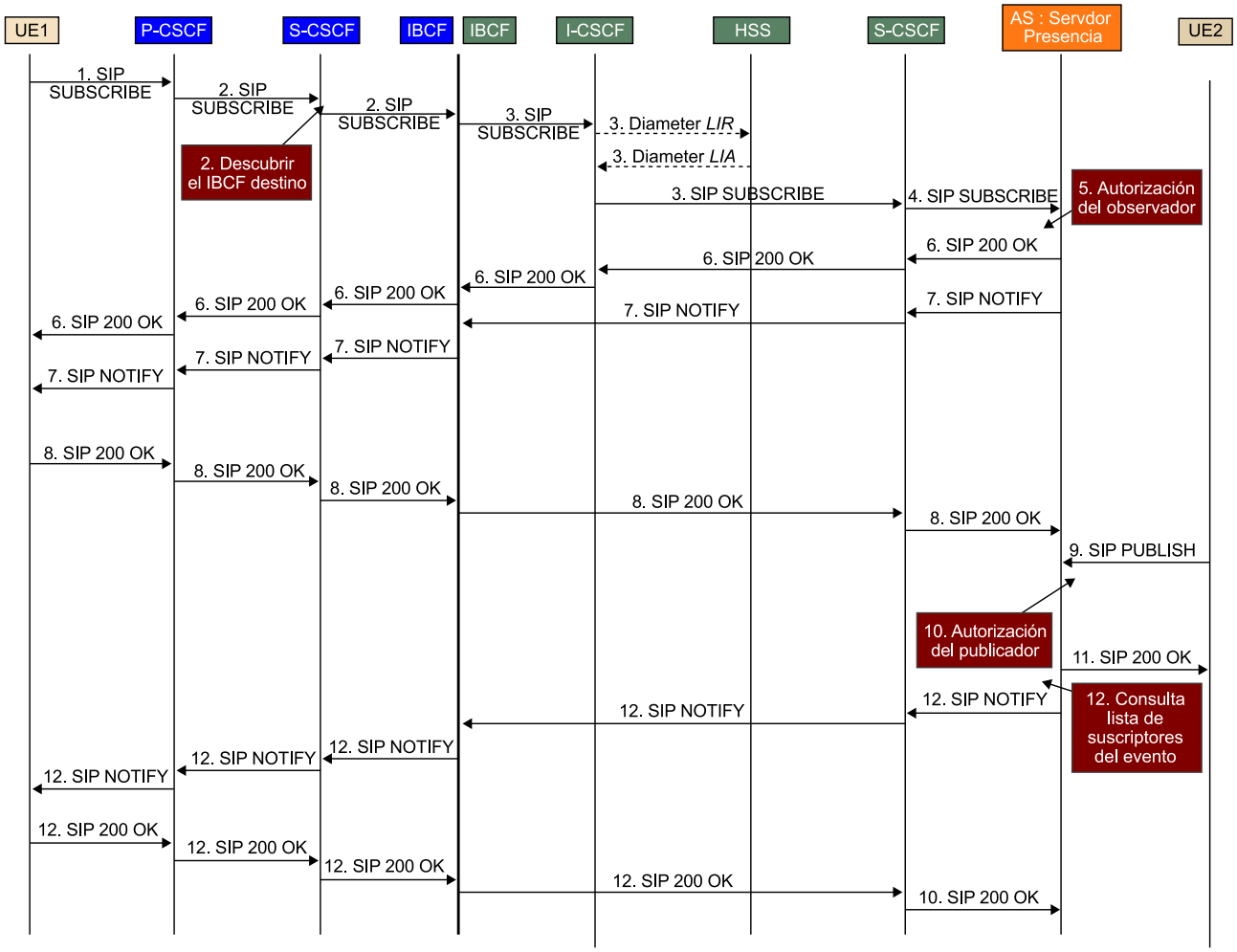
Nota

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.

4.2.2. 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 23, paso a paso los mensajes involucrados en este servicio.

Figura 23. Flujo de mensajes SIP en servicio de presencia



a) 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.

b) Paso 2: el mensaje SIP SUBSCRIBE pasa por el P-CSCF, que lo hace llegar al S-CSCF asignado al UE dentro del dominio. Este 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.

c) 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.

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

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

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

g) 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.

h) 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 al AS de presencia tu 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:

i) Paso 9: un UE externo cambia su información de presencia a 'No Disponible'. Entonces 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).

j) 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.

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

l) 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).

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 nuevo 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).

En el segmento de las redes de transporte de acceso como LTE, Wi-Fi, Wimax o ADSL, es donde se producen casos de contienda entre los equipos de usuario en el acceso a servicios contratados con capacidad garantizada. Por esta razón, en estas redes se requiere un mayor control de los recursos.

A pesar de que la tecnología relacionada con cada red de acceso (inalámbrica y cableada) es muy particular (tanto en mecanismos de adhesión a la red y asignación de dirección IP, como de solicitud de recursos) las distintas entidades de estandarización gubernamentales han querido ofrecer un modelo de referencia avanzado en la gestión de recursos que desvincule en lo posible estos dos aspectos:

- Los parámetros de QoS y SLA (acuerdos contractuales a nivel de aplicación) de los servicios.
- Aspectos concretos de la tecnología en capa 2 de la red de transporte (acceso y troncal).

En la **capa de transporte**, independientemente del modelo de referencia, siempre se identifica una **subcapa de procesado de transporte** en la que se implementan los mecanismos de garantía de QoS (aplicación de políticas de QoS particulares a cada usuario) y los de asignación de recursos (tanto en términos de capacidad en bits por segundo como en uso de direccionamiento IP público en NAT o NAPT). Posteriormente se identifica una **subcapa de control de transporte** en la que radica la inteligencia en el control de acceso a la red de transporte y sus recursos. En esta subcapa se distinguen dos grandes grupos de funciones: las que gestionan la adhesión a la red de acceso del UE y las que gestionan las solicitudes de recursos de QoS por parte del UE o de la propia capa de servicio.

En estos modelos de referencia se describen bloques o entidades funcionales y puntos de referencia o interfaces que los interconectan. Las entidades funcionales se describen con unas funciones concretassegún el modelo de referencia. Los puntos de referencia se describen por la información o parámetros que

intercambia cada entidad funcional con su entidad adyacente. Los puntos de referencia pueden ser implementados con protocolos concretos. Las entidades de estandarización recomiendan una lista de protocolos para facilitar la implementación de los puntos de referencia.

Dentro de la tarea de especificación, entidades como el 3GPP, ETSI-TISPAN y la ITU-T han contribuido muy activamente a proporcionar modelos de referencia para las distintas subcapas. En la siguiente tabla se resume la nomenclatura de las entidades funcionales más importantes de dichos modelos para las redes de transporte.

Tabla 3. Tabla resumen de entidades funcionales de modelos de referencia NGN para capa de transporte

		ITU-T	ETSI-TISPAN	3GPP
Subcapa de procesado de transporte	Control de acceso, traducción de direccionamiento y puertos	PE-FE	BGF	PCEF
	Aplicación de políticas de asignación de recursos.	TRE-FE	RCEF	
Subcapa de control de transporte	Adhesión a la red de acceso	NACF	NASS	(LTE) MME/ SPR
	Control de admisión y recursos	RACF	RACS	PCRF
	Punto de decisión final	PD-FE	SPDF	
	Control de admisión de perfil de usuario y recursos	PD-FE / TRC-FE	A-RACF	
Puntos de Referencia (Interfaces)	Función de aplicación (AF) Control de admisión y recursos.	Rs (Diameter)	Gq' (Diameter)	Rx (Diameter)
	Punto decisión finalControl admisión de perfil y recursos	Rt (Diameter)	Rq (Diameter)	
	Control de admisión de perfil de usuario y recursosSubcapa de procesado de transporte (aplicación de políticas de asignación de recursos)	Rn (sin especificar), Rc (SNMP o COPS)	Re (Diameter)	Gx (Diameter)
	Punto decisión finalSubcapa de procesado de transporte (control de acceso, traducción de direccionamiento y puertos)	Rw (Diameter o H.248)	Ia (H.248)	
	Adhesión a la red de accesoControl de admisión y recursos	Ru (Diameter)	e4 (Diameter)	Sp (Diameter)

Para implementar las interfaces que se definen en la tabla anterior, las diferentes entidades de estandarización proponen una serie de protocolos, incluyendo los mensajes a utilizar y sus respectivos parámetros. Vemos que el protoco-

lo predominante es el Diameter, compuesto por una serie de mensajes (también llamados *comandos*), que están formados por pares de atributos-valores (o AVP) que contienen información variada que afecta a la descripción de solicitud de QoS.

Respecto a la **capa de servicio**, las distintas entidades de estandarización definen sus propios subsistemas o componentes para definir los servicios multimedia que requieren garantía de QoS extremo a extremo. No obstante, hay un subsistema común en todas las entidades, el que defineel núcleo IMS, el cual fue definido por el 3GPP y adoptado como parte de los modelos de referencia de la capa de servicio para el resto de entidades de estandarización.

El **núcleo IMS** 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, videoconferencia o IPTV) sirviéndose 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 (voz o videoconferencia) o servidor de aplicación o AS (IPTV).

Aparte de servicios multimedia, IMS permite otros servicios sin componentes de tráfico multimedia, pero igualmente importantes, como mensajería instantánea o presencia.

Los elementos que componen las funciones de usuario, la capa de servicio y la capa de transporte colaboran e intercambian información para establecer sesiones de servicios y garantizar los recursos necesarios. En esta colaboración se definen dos tipos de mecanismos según quién dispare la reserva de recursos en la capa de transporte. El modo *push*, el AF (en este caso el núcleo IMS) inicia la reserva a través de un único punto de contacto con la capa de transporte (usando interfaces Rs, Rx o Gq') y el modo *pull*, donde es la propia red de acceso la que solicita estos recursos a la subcapa de procesado de transporte.

Las redes NGN plantean un nuevo marco en el que no solo se ofrecen los servicios actualmente presentes (voz, TV, mensajería, etc.), sino que dejan el terreno preparado para la inclusión de nuevos servicios futuros sin necesidad de realizar un cambio arquitectural y tecnológico en las redes de transporte (con los costes que ello conllevaría).

Ejercicios de autoevaluación

1. Un suscriptor A dispone en su domicilio de un PC con software multimedia (cliente IMS) así como una TV con capacidad de IPTV (cliente IMS con conectividad LAN). Además dispone de un fax que funciona con línea telefónica tradicional. Este suscriptor ha decidido aceptar la oferta de un operador con infraestructura IMS. Implica la instalación de una pasarela residencial a través de su conexión ADSL existente. Responded a las siguientes preguntas:

a) ¿Desde el punto de vista de la red de acceso, qué representa al equipo de usuario o UE?

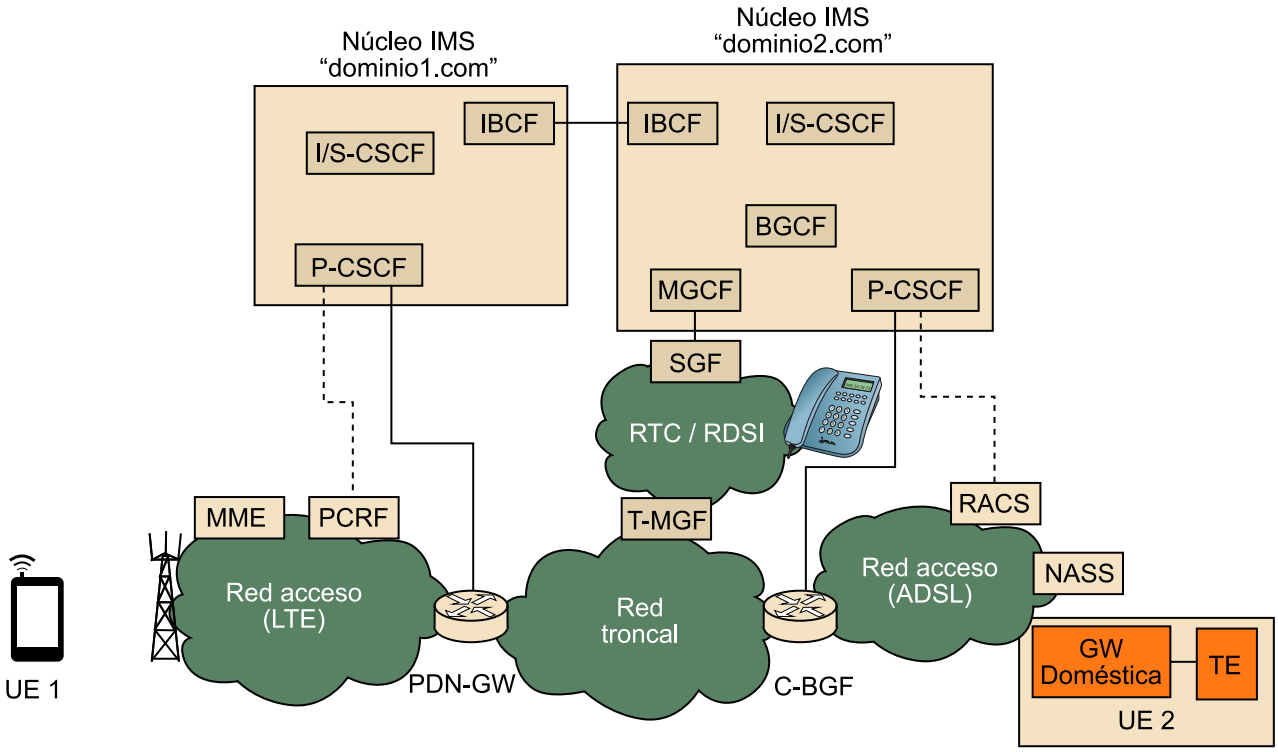
b) A nivel de asignación de adhesión a la red, ¿qué papel creéis que puede jugar la pasarela residencial?

c) ¿Cómo se integra el fax en este entorno y qué impacto tendría en la estructura funcional de la pasarela residencial?

d) ¿Qué alternativas ofrece IMS al uso de un fax analógico?

2. Dado el siguiente diagrama:

Figura 24. Diagrama ejercicio 2



Tenemos un UE 1 registrado en el núcleo IMS del dominio1.com (con dos IMPU: usuario1@dominio1.com y 674876321@dominio1.com) y un UE 2 registrado en el núcleo IMS del dominio2.com (con un IMPU: usuario2@dominio2.com). En este último caso, su dirección IP es privada (la asignada a la pasarela residencial). Contestad a las siguientes preguntas:

a) El UE 1 realiza una llamada de voz al UE 2. Identificad y mostrad el recorrido que hacen la señalización SIP IMS y los flujos RTP en esta llamada.

b) Identificad los puntos críticos donde aplicar políticas de QoS para garantizar la calidad de servicio de la llamada anterior.

c) El UE 1 realiza una segunda llamada hacia un terminal de ISDN con número de destino 934112233. Identificad y mostrad el recorrido de la señalización y los flujos RTP. ¿Qué número de llamante verá el usuario que recibe la llamada?

d) Para las dos redes de acceso que aparecen en el diagrama, ¿qué modelo de reserva de recursos creéis que puede tener cada una: *push* o *pull*?

3. Veamos el caso de la itinerancia centrándonos en el modelo de referencia de la ITU-T. Responded a las siguientes preguntas:

a) Un usuario llega con un terminal inalámbrico a un tercer país. Imaginemos que el operador de esta red tiene un acuerdo de *roaming* con el operador original. Al encenderlo, la red de acceso (de tecnología compatible con el terminal) le solicita autenticación explícita a través de los mecanismos propios de la propia red de acceso en capa 2. Describid las interacciones entre el UE y los distintos bloques que componen el NACF visitado y el local para conseguir que dicho UE se autentique y consiga el direccionamiento IP, sin olvidar la interacción con el RACF.

b) Una vez el UE ha obtenido el direccionamiento IP, inicia la invocación de los servicios IMS a través de su cliente. El operador de la red visitada no dispone de interconexión a su propio núcleo IMS. Especificad al menos un escenario de itinerancia en el que intervenga algún mecanismo de reserva de recursos en la red visitada.

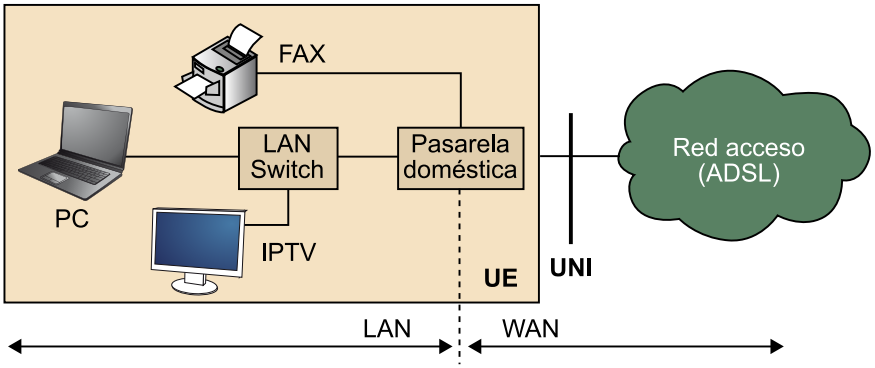
c) Imaginemos esta vez que el UE está en una red visitada operada por un operador y que posee interconexión con un núcleo IMS de dominio "visiteddomain.com". El UE quiere acceder a un servicio IMS de IPTV (Application Function) que solo es proporcionado vía el núcleo IMS de "homedomain.com". ¿Cómo se realiza la interconexión entre las redes de ambos operadores (visiteddomain.com y homedomain.com)?

Solucionario

Ejercicios de autoevaluación

1. a) El UE estaría formado por la propia pasarela residencial junto con todos los equipos conectados tras ella (PC, IPTV y fax).

Figura 25. Solucionario ejercicio 1a



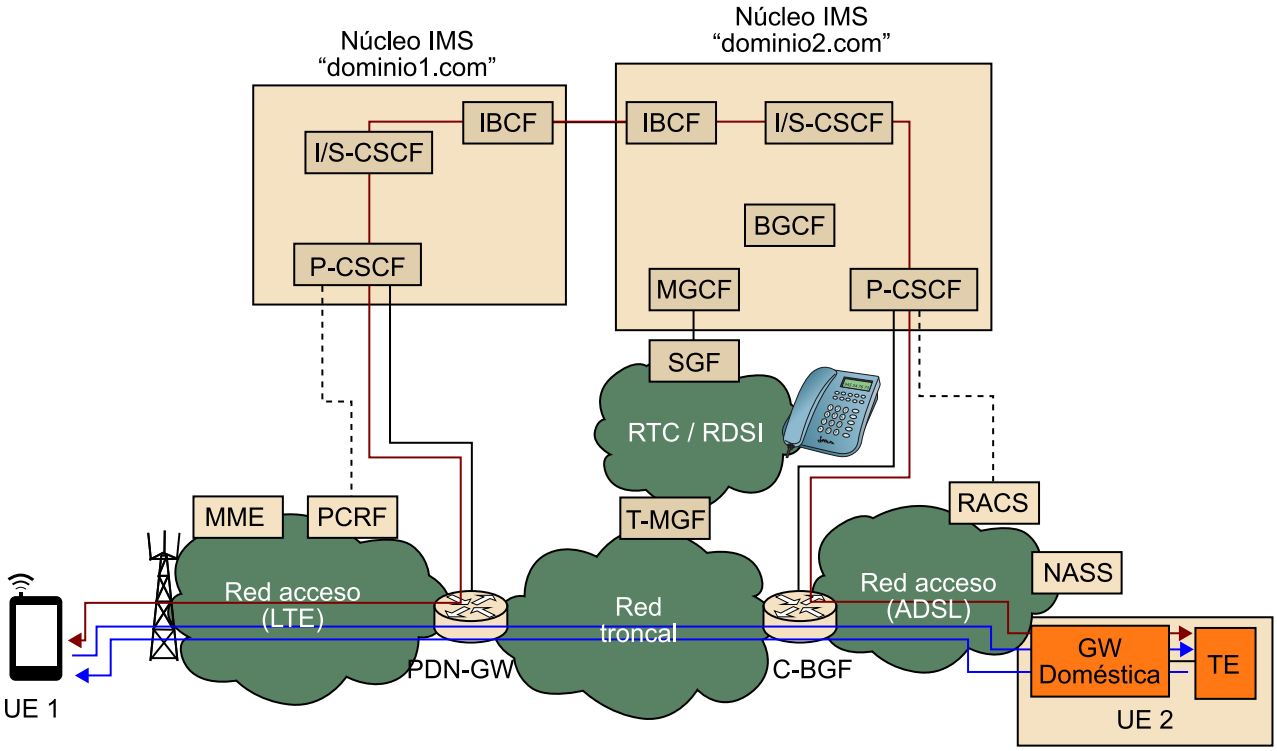
b) En el proceso de adhesión a la red, se observan dos zonas separadas por la pasarela residencial: la zona LAN, donde están conectados todos los dispositivos y la zona WAN que interconecta a la pasarela con la red de acceso. A nivel de autenticación, la pasarela puede realizar por el lado WAN su propia autenticación contra la red de acceso usando su ISIM con información de autenticación del suscriptor. Por el lado LAN puede participar en la autenticación de los dispositivos conectados a ella ya sea autenticando localmente a los dispositivos o, en el caso de que un dispositivo disponga de su propia ISIM, ejerciendo el reenvío de los mensajes al NACF o NASS. A nivel de asignación de dirección IP, la pasarela ejercería de servidor DHCP asignando un rango de IP privadas en el lado LAN. Por el lado WAN, la pasarela recibiría una dirección IP pública, asignada por los bloques funcionales correspondientes del NASS/NACF. Esta IP pública la puede utilizar para funciones de NATP.

c) El fax es un dispositivo que no tiene por qué disponer de conectividad LAN. Su interfaz es el mismo que un teléfono analógico. Con lo cual ya tenemos un primer impacto en la pasarela, que debe disponer de puertos FXS para que se pueda interconectar dicho fax. Además, la pasarela debe ejercer de intermediario entre dicho dispositivo y la red NGN generando la señalización SIP (IMS) debidamente sincronizada con el descuelgue del fax para el establecimiento de la llamada con la red RTC/ISDN pasando por los elementos del núcleo IMS. Se puede decir que cumple con parte de las funciones que se asignan a la AMG-FE de la ITU-T (sin contar la interconexión con AGC-FE) y cumple exactamente con la funcionalidad del R-MGF de la ETSI-TISPAN. Así pues, la pasarela ejerce de intermediario utilizando la identidad IMS (un IMPU dedicado para el fax) almacenada en su ISIM.

d) IMS ofrece un servicio de interconexión con las redes RTC/ISDN. El operador del cual es suscriptor debe proporcionar dicha interconexión (vía el bloque MGCF para señalización en el establecimiento de llamada y T-MGF/TMG-FE/IMS-MGW para el tráfico útil). Pero para poder invocar este servicio de fax, el PC debería tener el cliente de fax debidamente integrado con el cliente IMS para que a través de la interfaz Gm envíe la señalización SIP/SDP al núcleo IMS.

2. a) El siguiente diagrama muestra por dónde va la señalización IMS (en rojo) y los flujos RTP (en verde) con la voz. Se puede apreciar la independencia de la arquitectura para señalización SIP y RTP.

Figura 26. Solucionario ejercicio 2a

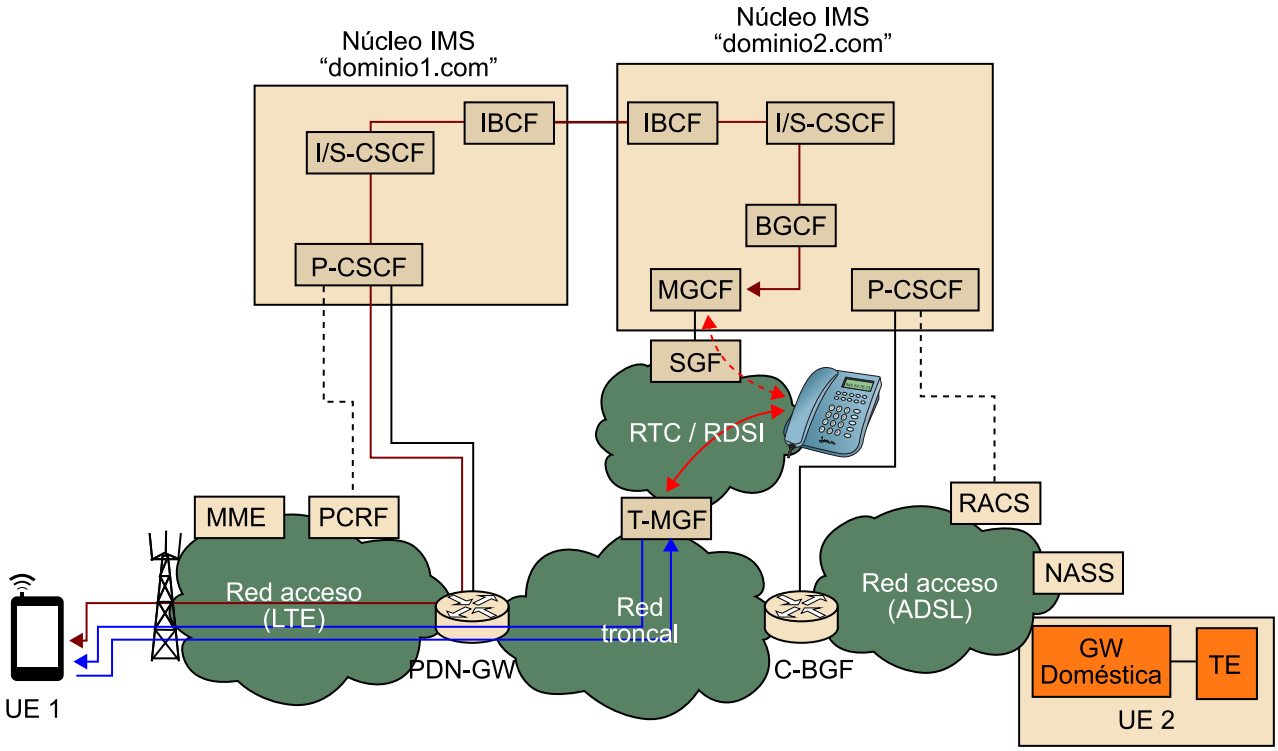


b) En el lado del UE 1, el PCRF aplica las reglas PCC sobre la PDN-GW, la cual establece los IP-CAN bearers entre el UE 1 y la PDN-GW. Con lo cual hay un punto para el tráfico en sentido UE 1 → UE 2, donde se deben mapear los flujos de datos de servicios. Éste es crítico para meter los paquetes por el IP-CAN correcto: el UE 1. La señalización SIP debe meterla por el IP-CAN preestablecido y dedicado con QCI explícito para señalización IMS y el flujo RTP debe introducirse por el IP-CAN establecido dinámicamente para tal servicio. El otro punto crítico en el lado del UE 1 es la PDN-GW, donde la señalización IMS y el flujo RTP en sentido UE 2 a UE 1 se mapea a los IP-CAN bearer correctos (Según su QCI).

En el lado del UE 2, el RACS aplica las políticas de servicio sobre la red ADSL para garantizar la QoS. El RACS configura el C-BGF para posibilitar la traducción NATP para los flujos RTP entrantes y salientes. La propia pasarela residencial también juega un papel importante en la garantía de QoS en sentido UE 2UE 1, ya que se produce un cuello de botella en su interfaz WAN. Es necesario resaltar la importancia de priorizar la señalización IMS por encima de cualquier otro tráfico para evitar retardos en el establecimiento de la llamada.

c) El siguiente diagrama muestra por dónde va la señalización IMS (en rojo) y los flujos RTP (en verde) con la voz. Se puede ver cómo el núcleo IMS del dominio1.com no encamina la llamada hacia su MGCF sino que la encamina al dominio2.com para que éste la saque por su MGCF. La razón por la que esto es así es arbitraria (políticas de encaminamiento de llamada en el dominio1.com).

Figura 27. Solucionario ejercicio 2c



El número llamante que verá el usuario en la RDSI será el del IMPU del UE 1: 674876321, ya que es de tipo Tel URI y el único compatible con RDSI.

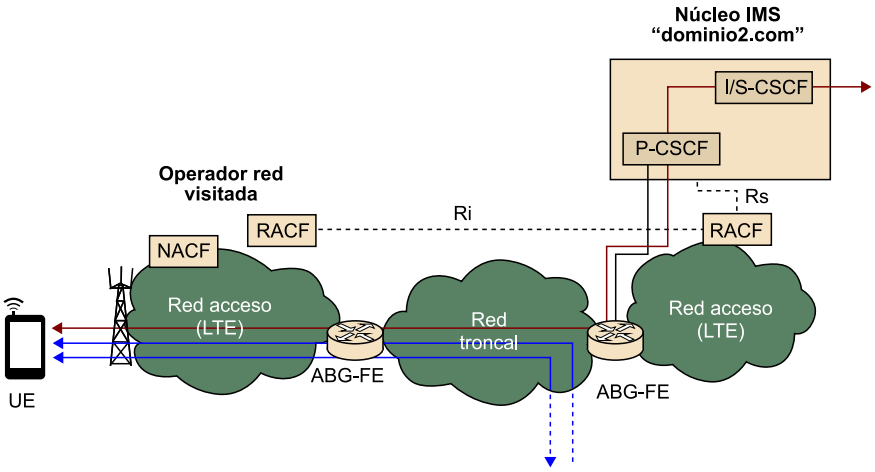
d) La red LTE puede tener tanto pull como push, dependiendo de quien inicie el establecimiento del IP-CAN bearer. En cambio, para el caso del ADSL vemos más probable que sea en modo push.

3. a) El UE solicita el establecimiento de una conexión en capa 2, que es recibida por el AR-FE, el cual reenvía dicha solicitud al AM-FE. El AM-FE detecta dicho intento de establecimiento de conexión, de la cual obtiene los identificadores de canal lógico de capa 2 que el UE está usando. Además reenvía la petición al TAA-FE para que éste inicie el reto de autenticación del UE. El UE recibe dicho reto y presenta las credenciales (IMPI) en la respuesta. El TAA-FE de la red visitada detecta (a partir del IMPI) que el dominio indicado no es el suyo. Por consiguiente, el TAA-FE de la red visitada localiza al TAA-FE de la red local (vía DNS con el dominio indicado en el IMPI) y actúa como proxy para reenviar el mensaje al TAA-FE local. Para ello utiliza la interfaz Ni, que está definido para tal propósito. A partir de entonces, el proceso de autenticación se realiza entre el UE y el TAA-FE local pasando por el TAA-FE visitado a modo de proxy. Cuando el usuario ha sido autenticado, el TAA-FE visitado envía la información de perfil de QoS recibida del TAA-FE local al TLM-FE.

El UE solicita direccionamiento IP al NAC-FE visitado, el cual se lo asigna y transfiere dicha información al TLM-FE para que lo asocie con la información de perfil. Una vez el TLM-FE tiene toda esta información, lo vuelca al RACF vía la interfaz Ru.

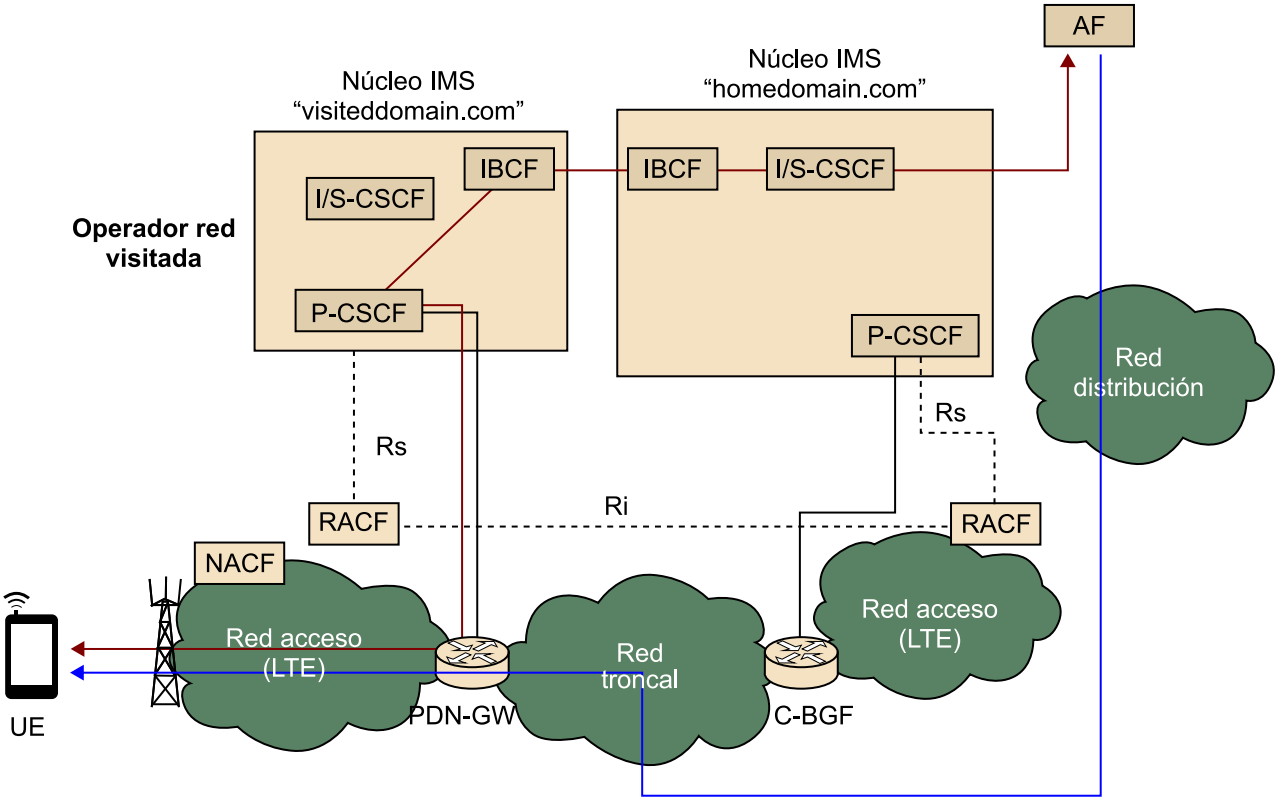
b) La siguiente figura muestra la interconexión de ambos operadores. Cabe destacar la interfaz Ri, que se utiliza para comunicar dos RACF (en realidad, dos PD-FE) entre sí de distintos dominios, como es este caso. Los mensajes SIP llegarían hasta el núcleo IMS “homedomain.com” a través de la red de acceso LTE del operador visitado pasando por la red troncal de interconexión. Cualquier petición de autorización de recursos desde el P-CSCF vía la interfaz Rs sería reenviada desde el RACF local hasta el visitado por la interfaz Ri.

Figura 28. Solucionario ejercicio 3b



c) En este caso, la interconexión entre ambas redes se podría realizar a través de los propios núcleos IMS. La señalización IMS del UE viajaría por la red de acceso visitada hasta el núcleo IMS visitado (visiteddomain.com), pasando por el P-CSCF y el IBCF directamente (sin pasar por el S-CSCF del dominio visitado). La interconexión directa entre P-CSCF y el IBCF es la interfaz Mx. De esta manera la señalización IMS llega hasta el “homedomain.com” donde llega hasta el correspondiente S-CSCF (via el I-CSCF) y de éste el AF. Éste entrega el contenido (canal de TV) a través de una red de distribución dedicada a tal fin (línea verde). Ni la red de acceso local ni el RACF local juegan ningún papel. La reserva de recursos en la red visitada se puede realizar vía el RACF correspondiente. El siguiente diagrama muestra esta interconexión.

Figura 29. Solucionario ejercicio 3c



Cabe mencionar que los IBCF, tanto de “visiteddomain.com” como “homedomain.com”, pueden controlar pasarelas entre redes troncales (IBG-FE) donde se pueden configurar traducciones NAT si fuera necesario.

Glosario

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

AAA Authentication, Authorization and Accounting. Protocolo de seguridad en redes IP.

ABG-FE Access Border Gateway Functional Entity. Función de pasarela fronteriza con red de acceso, dentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte (red troncal).

ADSL Asymmetric Digital Subscriber Line. Tecnología de la familia xDSL en la cual la capacidad del enlace ascendente es inferior que la capacidad del enlace descendente.

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 decontrol de transporte. Elemento definido por la ETSI-TISPAN.

AGC-FE Access Gateway Control Functional Entity. Control de pasarela de acceso en el modelo de referencia de la ITU-T para la capa de control de servicio. Controla una o varias AMG-FE.

ALG Application Level Gateway. En colaboración con un NAT/NATP, es un elemento que se encarga de traducir las direcciones IP que se encuentran en protocolos por encima de la capa 3. Cada protocolo necesita de su ALG (por ejemplo, FTP ALG o SIP ALG).

AMF Access Management Function. Función de gestión de acceso en el modelo de referencia del NASS de la ETSI-TISPAN.

AM-FE Access Management Functional Entity. Función de gestión de acceso en el modelo de referencia del NACF de la ITU-T.

A-MGF Access Media Gateway Function. Funcionalidad de pasarela de medios con dispositivos de usuario de telefonía tradicional en el modelo de referencia de la ETSI-TISPAN para la subcapa de procesado de transporte.

AMG-FE Access Media Gateway Functional Entity. Función de pasarela de medios de red acceso dentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte.

AN-FE Access Node Functional Entity. Función nodo de acceso dentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte.

ARF Access Relay Function. Función retransmisión de red de acceso que interactúa con el NASS del modelo de referencia de la ETSI-TISPAN.

AR-FE Access Relay Functional Entity. Función retransmisión de red de acceso que interactúa con el NACF del modelo de referencia de la ITU-T.

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.

ATM Asynchronous Transfer Mode. Red de transferencia asíncrona.

AUC Authenication Center. En el mundo de la telefonía móvil, es una base de datos para controlar a os móviles que se encuentran en su área de influencia.

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.

BBERF Bearer Binding and Event Reporting Fnction. Function 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.

BGF Border Gateway Function. Función de pasarela fronteriza, utilizada en la subcapa de procesado de transporte en el modelo de referencia de la ETSI-TISPAN.

BTF Basic Transport Function. Función básica de transporte, utilizada en la subcapa de procesado de trasnporte en el modelo de referencia de la ETSI-TISPAN.

C-BGF Core Border Gateway Function. Función de de pasarela fronteriza entre la red de acceso y la red troncal, utilizada en la subcapa de procesado de transporte en el modelo de referencia de la ETSI-TISPAN.

CD&LC-FE Delivery Control and Location Control Functional Entity. Componente de la subcapa de distribución de contenidos de la ITU-T que realiza la función de control de entrega de información y de la localización de la distribución del contenido.

CDC-FE Content Delivery Control Functional Entity. Componente de la subcapa de distribución de contenidos de la ITU-T que realiza la función de control de distribución de contenidos.

CDP-FE Content Delivery Processing Functional Entity. Componente de la subcapa de distribución de contenidos de la ITU-T que realiza la función almacenaje del contenido, procesamiento de este bajo control del CPR-FE y distribución del contenido a otras instancias del CDP-Fes bajo control del CD&LC-FE.

CGPD-FE Customer Gateway Policy Decision Functional Entity. Elemento localizado en la pasarela residencial para tomar decisiones sobre la aplicación de políticas de QoS en colaboración con el RACF. Esta entidad pertenece al modelo de referencia de la ITU-T.

CGPE-FE Customer Gateway Policy Enforcement Functional Entity. Elemento localizado en la pasarela residencial para instalar políticas de QoS desde el RACF. Esta entidad pertenece al modelo de referencia de la ITU-T.

CLF Connectivity session Location and repository Function. Función de gestión de localización en transporte (red de acceso) en el modelo de referencia del NASS de la ETSI-TISPAN.

CNGCF Customer Network Gateway Configuration Function. Función de configuración remota de la pasarela residencial dentro del modelo de referencia del NASS de la ETSI-TISPAN.

COPS Common Open Policy Service. Especifica un modelo simple cliente/servidor definido por el IETF para soportar el control de políticas sobre los protocolos de señalización de QoS.

CPE Customer Premises Equipment. Equipo dispositivo de cliente.

DHCP Dynamic Host Configuration Protocol. Protocolo de control de host dinámico.

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

DiffServ Servicios Diferenciados. Arquitectura de QoS en IP basada en dar un trato diferenciado a los paquetes según unas clases de servicio previamente fijadas.

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

ECF Elementary Control Function. Función de control elementaldentro del modelo de referencia de la ETSI-TISPAN en la subcapa de control de transporte.

EC-FE Elementary Control Functional Entity. Función de control elementaldentro del modelo de referencia de la ITU-T en la subcapa de control de transporte.

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.

EFF Elementary Forwarding Functionl. Función de transferencia elementaldentro del modelo de referencia de la ETSI-TISPAN en la subcapa de procesado de transporte.

EF-FE Elementary Forwarding Functional Entity. Función de transferencia elementaldentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte.

ENUM E.164 Numbering Mapping. Mapeo de un número de teléfono con identificadores equivalentes de telefonía en Internet.

EPC Evolved Packet Core. Redtroncal 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. Definiciónde la red radio de LTE según el 3GPP.

FP Flow Point. Punto de flujo de entrada y salida de paquetes.

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

GERAN GSM Edge Radio Access. Definiciónde 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.

GSC-FE General Services Control Functional Entity. En el modelo de referencia de la ITU-t para la subcapa de control de servicios, este elemento proporciona una plataforma que da soporte a los futuros servicios que se planteen sobre redes de paquetes.

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.

HDC-FE Handover Decision Control Functional Entity. Función de control de decisión de traspaso de red dentro del modelo de referencia del MMCF de la ITU-T en la subcapa de control de transporte.

HGWC-FE Home Gateway Configuration Functional Entity. Función de configuración remota de la pasarela residencial dentro del modelo de referencia del NACF de la ITU-T.

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 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.

IBGC-FE Interconnection Border Gateway Control Functional Entity. Función de control de pasarela fronteriza con otra red de troncal, dentro del modelo de referencia de la ITU-T en la subcapa de control de servicio (red troncal).

I-BGF Interconnection Border Gateway Function. Función de de pasarela fronteriza entre dos redes troncales, utilizada en la subcapa de procesado de transporte en el modelo de referencia de la ETSI-TISPAN.

IBG-FE Interconnection Border Gateway Functional Entity. Función de pasarela fronteriza con otra red de troncal, dentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte (red troncal).

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.

I-CSC-FE Interrogating Call Session Control Functional Entity. Componente equivalente al I-CSCF del 3GPP pero en el modelo equivalente de la ITU-T.

IETF Responde a las siglas de 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. http://www.ietf.org

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 la provisión de servicios multimedia en telefonía móvil basado en los protocolos definidos por IETF, como 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.

IMS SSO IMS Single Sign-On. Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

IMS-MGF IMS Media Gateway Function. Funcionalidad de pasarela de medios con enlaces de red troncal de telefonía tradicional en el modelo de referencia del 3GPP para la subcapa de procesado de transporte.

IntServ Servicios Integrados. Arquitectura de QoS en IP basada en la reserva de recursos individualizada por cada servicio.

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 y una tarjeta smart card con información sobre la identidad de un usuario IMS.

ISUP Protocolo de circuitos conmutados, usado para configurar, manejar y gestionar llamadas de voz y datos sobre RTC y RDSI.

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 rede de próxima generación.

IWF Interworking Funcion. Elemento del modelo de referencia de la ETSI-TISPAN en la capa de control de servicio cuya función es adaptar o traducir la señalización de peticiones SIP hacia otros que no soportan el protocolo SIP de IMS.

L2HCF Layer 2 Handover Control Function Entity. Funcion de control de la movilidad en capa 2 dentro del MMFC en el modelo de referencia de la ITU-T.

L2HE-FE Layer 2 Handover Execution Function Entity. Funcion de ejecución de la movilidad en capa 2 en el modelo de referencia de la ITU-T para el procesado de transporte.

L3HCF Layer 3 Handover Control Function Entity. Funcion de control de la movilidad en capa 3 dentro del MMFC en el modelo de referencia de la ITU-T.

L3HEF Layer 3 Handover Execution Function.Funcion de ejecución de la movilidad en capa 3 en el modelo de referencia de la ITU-T para el procesado de transporte.

LTE Long Term Evolution. Definida por el 3GPP se considera la telefonía de 4G.

MAC Medium Access Control. Control de acceso al medio (capa 2).

MBR Maximum Bit Rate. Tasa de bit máxima (usado como parámetro de caraterización 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 y la ETSI-TISPAN en el núcleo IMS.

MGC-FE Media Gateway Control Functional Entity. Función de control de pasarela de medios en el modelo de referencia de la ITU-T en el control de transporte.

MGF Media Gateway Function. Funcionalidad de pasarela de medios con redes de circuitos tradicionales en el modelo de referencia de la ETSI-TISPAN para la subcapa de procesado de transporte.

MLM-FE Mobile Location Management Functional Entity. Función de gestión de localización móvil dentro del MMFC del modelo de referencia de la ITU-T en la subcapa de control de transporte.

MMCF Mobility Management Control Function. Función de control de la gestión de la movilidaden el modelo de referencia de la ITU-T.

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).

MPLS Multi-Protocol Label Switching. Tecnología que combina las ventajas del encaminamiento de nivel 3 con la rápida conmutación de nivel 2, utilizando la conmutación de paquetes para una etiqueta de longitud fija.

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

MRB-FE Multimedia Resource Broker Functional Entity. Función de gestión de recursos de medios en el modelo de la ITU-T en la subcapa de soporte a servicios y a aplicaciones.

MRC-FE Media Resource Control Functional Entity. Función de control de recursos de medios en el modelo de referencia de la ITU-T en el control de transporte.

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.

MRP-FE Media Resource Processing Functional Entity. Función de procesado de recursos de medios en el modelo de referencia de la ITU-T en el procesado de transporte.

MSC Mobile Switching Center. Central de conmutación móvil. Elemento de telefónica móvil GSM.

NACF (ETSI) Network Access Configuration Function. Función de asignación de direccionamiento IP en la red de acceso en el modelo de referencia del NASS de la ETSI-TISPAN.

NACF (ITU-T) Network Attachment Control Function. Conjunto de funciones que definen la adhesión a la red de acceso en el modelo de referencia de la ITU-T.

NAC-FE Network Access Configuration Functional Entity. Función de asignación de direccionamiento IP en la red de acceso en el modelo de referencia del NACF de la ITU-T.

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

NASS Network Attachment Subsystem. Conjunto de funciones que definen la adhesión a la red de acceso en el modelo de referencia de la ETSI-TISPAN.

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

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

NID-FE Network Information Distribution Functional Entity. Función de distribución de información de red dentro del MMFC en el modelo de referencia de la ITU-T.

NIR-FE Network Information Repository Functional Entity. Función de almacenaje de información de red dentro del MMFC en el modelo de referencia de la ITU-T.

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

NSIW-FE Network Signalling Interworking Funcional Entity. Elemento del modelo de referencia de la ITU-T en la capa de control de servicio cuya función es adaptar o traducir la señalización de peticiones SIP hacia otros que no soportan el protocolo SIP de IMS.

OCS On-line 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 Off-line 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.

OSPF Open Shortest Path First. Protocolo de encaminamiento IP dinámico basado en vector de coste.

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 (IMS). Es un elemento definido por el 3GPP.

P-CSC-FE Proxy Call Session Control Functional Entity. Componente equivalente al P-CSCF del 3GPP pero en el modelo equivalente de la ITU-T.

PDBF Profile Data Base Function. Entidad que almacena los perfiles de usuario a nivel de red de transporte en el modelo de referencia del NASSde la ETSI-TISPAN.

PD-FE Policy DecisionFunctional Entity. Funcion de decisión de políticas dentro del modelo de referencia de la ITU-T en la subcapa de control de transporte.

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

PE-FE Policy Enforcement Functional Entity. Función de aplicación de políticas dentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte.

PPP Point toPoint Protocol. Protocolo de capa 2 punto a punto.

PPPoE PPP over Ethernet.Protocolo PPP sobre Ethernet.

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

QCI QoS Class Identifier.parametros 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.

RACF (ITU-T) Resource and Admision Control Function. Grupos de funciones que conforman el control de admisión y recursos del modelo de referencia de la ITU-T.

RACS Resource and Admision Control Subsystem. Grupos de funciones que conforman el control de admisión y recursos del modelo de referencia de la ETSI-TISPAN.

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.

RCEF Resource Control Enforcement Function. Función de aplicación de control de recursos y aplicación de políticas de QoS desde el RACS. Es un elemento perteneciente al modelo de referencia de la ETSI-TISPAN.

RDSI Red Digital de Servicios Integrados.

RFC Responde a las siglas de Request For Comment y es donde se plasma por escrito los estándares que define la IETF.

RIP Routing Information Protocol. Protocolo de encaminamiento IP dinámico basado en vector distancia.

RSVP Resource Reservation Protocol. Protocolo de la capa de transporte diseñado para reservar recursos de una red bajo la arquitectura de servicios integrados (IntServ).

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 ArchitectureEvolution. 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).

SCF Service Control Functions. Es la manera que el modelo de referencia de la ITU-T llama al conglomerado de entidades funcionales que conforman la capa de control de servicio (por ejemplo, el núcleo IMS).

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.

S-CSC-FE Serving Call Session Control Functional Entity. Componente equivalente al S-CSCF del 3GPP pero en el modelo equivalente de la ITU-T.

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

SGF Signalling Gateway Function. Función de pasarela de señalización a redes de circuitos en el modelo de referencia de la ETSI-TISPAN en el procesado de transporte.

SG-FE Signalling Gateway Functional Entity. Función de pasarela de señalización a redes de circuitos en el modelo de referencia de la ITU-T en el procesado de transporte.

SGSN/GGSN Serving GPRS Support Node/Gateway GPRS Support Node. En una red troncal GPRS el SGSN se encarga de la parte 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 movil), 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 Responde a las siglas de Service Level Agreement y define las características del servicio para un usuario que es 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.

SNMP Simple Network Management Protocol.Protocolo para la monitorización y control remotos de elementos de red definido por el IETF. Está basado en la consulta de bases de datos localizadas en cada dispositivo de red llamada MIB o Management Information Base.

SPDF Service Policy Decision Function. Funcion deecisión de la política de servicio dentro del RACS en el modelo de referencia de la ETSI-TISPAN.

SPR Subscription Profile Repository. Funcion 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.

SUP-FE Service User Profile Functional Entity. 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 de la ITU-T).

TAA-FE Transport Authentication and Authorization Functional Entity. Función de autenticación y autorización en la red de transporte (red de acceso) en el modelo de referencia del NACF de la ITU-T.

Tabla MAC En un switch, es la tabla en la que se relaciona puerto físico y dirección de hardware (también llamada dirección MAC).

TCP Transport Control Protocol.

TDM Time Division Multiplex

TDMA Time Division Multiple Access. Reparticion de recursos de transmission por multiplexación de tiempo.

TE Terminal Equipment o terminal de usuario.

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 tipología de la red.

TISPAN Responde a las siglas de TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) y SPAN (Services and Protocols for Advanced Networks). Es una organización fundada por la ETSI para la estandarización de redes fijas y convergencia con Internet.

TLM-FE Transport Location Management Functional Entity. Función de gestión de localización en transporte (red de acceso) en el modelo de referencia del NACF de la ITU-T.

T-MGF Trunk Media Gateway Function. Funcionalidad de pasarela de medios con enlaces de red troncal de telefonía tradicional en el modelo de referencia de la ETSI-TISPAN para la subcapa de procesado de transporte.

TMG-FE Trunking Media Gateway Functional Entity. Función de pasarela de medios de red de circuitos dentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte (red troncal).

ToS Type of Service. Parámetro que indica el tipo de servicio incluido en la cabecera IP.

TRC-FE Transport Resource Control Functional Entity. Función de control de recursos de transporte dentro del modelo de referencia de la ITU-T en la subcapa de control de transporte.

TRE-FE Transport Resource Enforcement Functional Entity. Función de aplicación de recursos de transporte dentro del modelo de referencia de la ITU-T en la subcapa de procesado de transporte.

TrGW Transition Gateway. Función de de pasarela fronteriza entre dos redes troncales, utilizada en la subcapa de procesado de transporte en el modelo de referencia del 3GPP.

TUP-FE Transport User Profile Functional Entity. Entidad que almacena los perfiles de usuario a nivel de red de transporte en el modelo de referencia del NACF de la ITU-T.

UAAF User Authentication and Authorization Function. Función de autenticación y autorización del usuario en la red de transporte (red de acceso) en el modelo de referencia del NASS de la ETSI-TISPAN.

UDP User Datagram Protocol. Protocolo de capa 4 para el envio de paquetes sin confirmación.

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

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.

UPSF User Profile Subscription Function. 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 de la ETSI-TISPAN).

URI Uniform Resource Identifier. Esquema de identificación de usuario.

USIW-FE User Signalling Interworking Funcional Entity. Elemento del modelo de referencia de la ITU-T en la capa de control de servicio cuya función es adaptar o traducir la señalización de todos aquellos terminales de usuario que no soportan el protocolo SIP de IMS.

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

VLAN ID Virtual Local Area Network Identifier. Identificador de red local virtual, utilizado en un switch para dividirse en varios switches virtuales con menos bocas.

VoIP Voice over IP. Servicio de voz que se ofrece sobre una red de conmutación de paquetes basada en el protocolo.

WiMAX Worldwide interoperability for Microwave Access. Conjunto de estándares de redes metropolitanas inalámbricas de la familia IEEE 802.16.

xDSL x Digital Subscriber Line. Familia de tecnologías de acceso a Internet de banda ancha basadas en la digitalización del bucle de abonado telefónico.

XML eXtensible Markup Language. Es un lenguaje de marcas desarrollado por el World Wide Web Consortium (W3C) permitiendo definir la gramática de lenguajes específicos para estructurar documentos grandes.

x-RACF Resource and Admission Control Function. Función perteneciente al RACS dentro del modelo de referencia de la ETSI-TISPAN encargado del control de los recursos de la red de transporte (A-RACF aplica a la red de acceso y C-RACF a la red troncal).

Bibliografía

ITU-T Recomendación Y.2012 (04/2010). *Functional requirements and architecture of next generation networks*.

ITU-T Recomendación Y.2014 (03/2010). *Network attachment control functions in next generation networks*.

ETSI-TISPAN Recomendación ES 282 004 v3.4.1 (2010-03). *NASS Functional Architecture*.

ETSI-TISPAN Recomendación TS 183 020 v1.1.1 (2006-03). *NASS - Roaming in TISPAN - Interface Protocol Definition*.

ITU-T Recomendación Y.2111 (11/2011). *Resource and admission control functions in next generation networks*.

ETSI-TISPAN Recomendación ES 282 003 v3.5.1 (2011-04). *RACS Functional Architecture*.

ITU-T Recomendación Y.2018 (09/2009). *Mobility management and control framework and architecture within the NGN transport stratum*.

3GPP Recomendación TS 23.203 v11.5.0 (2012-03). *Policy and charging control architecture*.

ETSI-TISPAN Recomendación ES 282 001 V3.4.1 (2009-09). *NGN Functional Architecture*.

ETSI-TISPAN Recomendación ES 123 517 8.0.0 (2007-12). *IP Multimedia Subsystem*.

3GPP Recomendación TS 23.228 v11.4.0 (2012-03). *IP Multimedia Subsystem (IMS)*.

3GPP Recomendación TS 29.214 v11.0.0 (2011-03). *Policy and Charging Control over Rx reference point*.

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

Anexo

Resumen de puntos de referencia del modelo de referencia de la ITU-T

A continuación vamos a mostrar un resumen de todos los puntos de referencia que aparecen en la arquitectura de referencia de la ITU-T que se han mostrado a lo largo de este documento.

1) Puntos de referencia del NACF

La siguiente tabla muestra una descripción de los puntos de referencia que menciona la ITU-T y su recomendación sobre el protocolo para implementarlo.

Tabla 4. Puntos de referencia del NACF

Nombre	Entidades que interconecta	Protocolo	Descripción
T-U1	CPE y AR-FE	<sin especificar>	Utilizado por el CPE para iniciar sesión en capa 2.
TC-T1	AR-FE y AM-FE	<sin especificar>	Utilizado por el NACF para finalizar sesión capa 2 y detectar adhesión a la red de un CPE.
Na	AM-FE y TAA-FE	<sin especificar>	Utilizado por el AM-FE para intercambiar mensajes de proceso de autenticación del CPE.
Nd	AM-FE y NAC-FE	<sin especificar>	Utilizado por el AM-FE para intercambiar mensajes de asignación de dirección IP.
Nb	TAA-FE y TUP-FE	<sin especificar>	Utilizado por el TAA-FE para acceder a la base de datos de perfiles QoS y credenciales.
Ni	TAA-FE (proxy) y TAA-FE	<sin especificar>	Utilizado por el TAA-FE (proxy) en la red visitada para acceder a la base de datos de perfiles QoS y credenciales de la red original.
Nc	TAA-FE y TLM-FE	<sin especificar>	Utilizado por el TAA-FE para transferir la información de suscripción de transporte del usuario autenticado.
Ne	NAC-FE y TLM-FE	<sin especificar>	Utilizado por el NAC-FE para transferir la información de asignación de direccionamiento IP y parámetros de identificación de red de acceso.
Ng	TLM-FE y TLM-FE	Diameter	Utilizado por el TLM-FE local para itinerancia.
Ru	TLM-FE y PD-FE(RACF)	Diameter	Utilizado para transferir información de identificación en red de acceso y perfil de QoS del usuario al RACF.
Nx	TLM-FE y HGWC-FE	Diameter	Utilizado para transferir información de suscripción e información de seguridad desde el TLM-FE a HGWC-FE.
S-TC1	TLM-FE y Funciones ControlServicio (SCF)	Diameter	Utilizado por el SCF para solicitar información de localización del usuario, así como reportar al SCF eventos relacionados con la adhesión del usuario en la red.
TC-Ux	HGWC-FE y CPE	<sin especificar>	Utilizado para la monitorización y configuración remota de la pasarela doméstica.

Nombre	Entidades que interconecta	Protocolo	Descripción
M1	TLM-FE y MLM-FE	<sin especificar>	Utilizado para transferir al MLM-FE parámetros de movilidad.
M2	TLM-FE y HDC-FE	<sin especificar>	Utilizado para transferir al HDC-FE parámetros de movilidad.
M13	TLM-FE y NID-FE	<sin especificar>	Utilizado para transferir al NID-FE parámetros de movilidad.

2) Puntos de referencia del NACF

La siguiente tabla muestra una descripción de los puntos de referencia que menciona la ITU-T y su recomendación sobre el protocolo o protocolos para implementarlo.

Tabla 5. Puntos de referencia del RACF

Nombre	Entidades que interconecta	Protocolo	Descripción
Rs	Funciones de Control de Servicio (SCF) y PD-FE	Diameter	Utilizado por el SCF para la solicitud de recursos de QoS y reporte de eventos de capa de transporte.
Ri	PD-FE y PD-FE	Diameter	Utilizado por un PD-FE de otro dominio para la solicitud de recursos de QoS y reporte de eventos de capa de transporte al PD-FE. También usado para itnerancia en la reserva de recursos.
Rd	PD-FE y PD-FE	Diameter	Utilizado por un PD-FE del mismo dominio para la solicitud de recursos de QoS y reporte de eventos de capa de transporte al PD-FE adyacente.
Rw	PD-FE y PE-FE	Diameter, H.248	Utilizado por el PD-FE para instalar políticas de QoS y usado por el PE-FE para solicitar recursos (modo *pull*).
Rt	PD-FE y TRC-FE	Diameter	Utilizado por el PD-FE para solicitar control de admisión al TRC-FE sobre disponibilidad de recursos.
Rp	TRC-FE y TRC-FE	Diameter	Utilizado por un TRC-FE del mismo dominio para la solicitud de control de admisión de recursos al TRC-FE adyacente.
Rn	TRC-FE y TRE-FE	<sin especificar>	Utilizado por el TRC-FE para aplicar las decisiones del control de admisión de disponibilidad de recursos.
Rc	TRC-FE y subcapa Procesado Transporte	COPS, SNMP	Utilizado por el TRC-FE para captar información de topología y estado de recursos de la red.
Ru	PD-FE y TLM-FE (NACF)	Diameter	Utilizado por el PD-FE para obtener del NACF información de suscripción.
Ro	PD-FE y HDC-FE (MMCF)	<sin especificar>	Utilizado por el HDC-FE para funciones de movilidad.
Rm	PD-FE y MPM	<sin especificar>	Utilizado para transferir información de monitorización al MPM.
Rh	PD-FE y CGPE-FE	COPS	Utilizado para instalar políticas de QoS en la pasarela residencial.
Rh’	PD-FE y CGPD-FE	<sin especificar>	Utilizado para solicitar control de admisión de recursos en la pasarela residencial.

3) Puntos de referencia del MMCF

La siguiente tabla muestra una descripción de los puntos de referencia que menciona la ITU-T y su recomendación sobre el protocolo para implementarlo.

Tabla 6. Puntos de referencia del MMCF

Nombre	Entidades que interconecta	Protocolo	Descripción
M1	TLM-FE y MLM-FE	<sin especificar>	Utilizado para transferir al MLM-FE parámetros de movilidad (p. ej. IP temporal asignada).
M2	TLM-FE y HDC-FE	<sin especificar>	Utilizado para transferir al HDC-FE parámetros de movilidad (p. ej. asociaciones de seguridad con el equipo de usuario).
M3	CPE y MLM-FE	<sin especificar>	Utilizado para transferir al MLM-FE actualizaciones de localización del CPE.
M4	CPE y HDC-FE	<sin especificar>	Utilizado por el CPE para notificar eventos de movilidad y utilizado por el enviar al CPE comandos desde el HDC-FE de indicación de cambio a otra red.
M5	CPE y NID-FE	<sin especificar>	Utilizado para el enviar al CPE comandos desde el NID-FE de información de redes candidatas.
M6	HDC-FE y L2HE-FE	<sin especificar>	Utilizado por el HDC-FE para ejecutar el *handover* en capa 2.
M7	HDC-FE y L3HE-FE	<sin especificar>	Utilizado por el HDC-FE para ejecutar el *handover* en capa 3.
M8, Ro	HDC-FE y PD-FE (RACF)	<sin especificar>	Utilizado por el HDC-FE para reservar recursos en la red de acceso cuando el equipo de usuario se mueve a otra red.
M9	MLM-FE y MLM-FE	<sin especificar>	Utilizado para intercambiar registros de movilidad entre dos MLM-FE.
M10	MLM-FE y HDC-FE	<sin especificar>	Utilizado para intercambiar indicaciones y notificaciones de *handovers*.
M11	HDC-FE yNID-FE	<sin especificar>	Utilizado por el HDC-FE para conseguir información sobre otras redes de acceso en las que realizar un *handover*.
M12	NID-FE y NIR-FE	<sin especificar>	Utilizado por el NID-FE para conseguir información sobre otras redes de acceso.
M13	TLM-FE y NID-FE	<sin especificar>	Utilizado para transferir al NID-FE parámetros de movilidad.

Resumen de puntos de referencia del modelo de referencia de la ETSI-TISPAN

A continuación vamos a mostrar un resumen de todos los puntos de referencia que aparecen en la arquitectura de referencia de la ETSI-TISPAN que se han mostrado a lo largo de este documento.

1) Puntos de referencia del NASS

La siguiente tabla muestra una descripción de los puntos de referencia que menciona la ETSI-TISPANpara el NASS y su recomendación sobre el protocolo para implementarlo.

Tabla 7. Puntos de referencia del NASS

Nombre	Entidades que interconecta	Protocolo	Descripción
e1	UE y ARF y AMF	<sin especificar>	Utilizado por el UE para iniciar sesión en capa 2 y detectar adhesión a la red de un UE.
a3	AMF y UAAF	<sin especificar>	Utilizado por el AMF para intercambiar mensajes de proceso de autenticación del UE.
a1	AMF y NACF	<sin especificar>	Utilizado por el AMF para intercambiar mensajes de asignación de dirección IP.
e5	UAAF (proxy) y UAAF	Radius	Utilizado por el UAAF (proxy) en la red visitada para acceder a la base de datos de perfiles QoS y credenciales de la red original.
a4	UAAF y CLF	<sin especificar>	Utilizado por el UAAF para transferir la información de suscripción de transporte del usuario autenticado.
a2	NACF y CLF	<sin especificar>	Utilizado por el NACF para transferir la información de asignación de direccionamiento IP y parámetros de identificación de red de acceso.
e2	CLF y CLF	Diameter	Utilizado por el CLF local para itinerancia.
e2	CLF y CNGCF	Diameter	Utilizado para transferir información de suscripción e información de seguridad desde el CLF a CNGCF.
e2	CLF y AF	Diameter	Utilizado por el AF para solicitar información de localización del usuario, así como reportar al AF eventos relacionados con la adhesión del usuario en la red.
e4	CLF y A-RACF (RACS)	Diameter	Utilizado para transferir información de identificación en red de acceso y perfil de QoS del usuario al RACS.
e3	CNGCF y CNG	<sin especificar>	Utilizado para la monitorización y configuración remota de la pasarela doméstica.

2) Puntos de referencia del RACS

La siguiente tabla muestra una descripción de los puntos de referencia que menciona la ETSI-TISPAN y su recomendación sobre el protocolo para implementarlo.

Tabla 8. Puntos de referencia del RACF

Nombre	Entidades que interconecta	Protocolo	Descripción
Gq'	AF y SPDF	Diameter	Utilizado por el AF para la solicitud de recursos de QoS y reporte de eventos de capa de transporte.
Ri'	SPDF y SPDF	Diameter	Utilizado por un SPDF de otro dominio para la solicitud de recursos de QoS y reporte de eventos de capa de transporte al SPDF. También usado para itinerancia en la reserva de recursos.
Rd'	SPDF y SPDF	Diameter	Utilizado por un SPDF del mismo dominio para la solicitud de recursos de QoS y reporte de eventos de capa de transporte al SPDF adyacente.

Nombre	Entidades que interconecta	Protocolo	Descripción
Ia	SPDF y BGF	H.248	Utilizado por el SPDF para instalar políticas de QoS en el BGF.
Rq	SPDF y x-RACF	Diameter	Utilizado por el SPDF para solicitar control de admisión al x-RACF sobre perfil de suscripción y disponibilidad de recursos.
Rr	x-RACF y x-RACF	Diameter	Utilizado por un x-RACF del mismo dominio para la solicitud de control de admisión de recursos al x-RACF adyacente.
Re	x-RACF y RCEF	Diameter	Utilizado por el x-RACF para aplicar las decisiones del control de admisión de disponibilidad de recursos.
e4	A-RACF y CLF (NASS)	Diameter	Utilizado por el A-RACF obtener del NASS información de suscripción.
Rf	(SPDF, x-RACF) y Funciones de Facturación	Diameter	Utilizado para transferir información de facturación.

3) Puntos de referencia del modelo PCC

La siguiente tabla muestra una descripción de los puntos de referencia que menciona el 3GPP y su recomendación sobre el protocolo para implementarlo.

Tabla 9. Puntos de referencia del modelo PCC

Nombre	Entidades que interconecta	Protocolo	Descripción
Rx	AF y PCRF	Diameter	Utilizado por el AF para la solicitud de recursos de QoS y reporte de eventos de capa de transporte.
S9	V-PCRF y H-PCRF	Diameter	Utilizado por un PCRF de otro dominio para la solicitud de recursos de QoS (visitado) para itinerancia en la reserva de recursos.
Gx	PCRF y PCEF	Diameter	Utilizado 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.
Gxx	PCRF y BBERF	Diameter	Utilizado 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.
Sp	PCRF y SPR	Diameter	Utilizado por el PCRF para obtener del SPR información de suscripción.
Gy	PCEF y OCS	Diameter	Utilizado para transferir información de facturación *on-line* (prepago).
Gz	PCEF y OFCS	Diameter	Utilizado para transferir información de facturación *off-line* (pospago).

4) Puntos de referencia del componente IMS

La siguiente tabla muestra una descripción de los puntos de referencia para el subsistema IMS que se mencionan en los modelos de la ITU-T, la ETSI-TISPAN y el 3GPP, así como la recomendación sobre el protocolo para implementarlo.

Tabla 10. Puntos de referencia del núcleo IMS

Nombre	Entidades que interconecta	Protocolo	Descripción
Gq', Rx y Rs (S-TC2, S-TC3, S-TC4, S-TC5)	P-CSCF (o IBCF para la ETSI) y control de admisión de recursos (RACF, RACS y PCRF)	Diameter	Utilizado por el P-CSCF (o también IBCF para la ETSI) para la solicitud de recursos de QoS y reporte de eventos de capa de transporte.
Gm y S-U1	UE y P-CSCF	SIP	Interfaz entre UE y P-CSCF para intercambiar mensajes de señalización SIP de IMS (registro, control de sesiones y transacciones).
Mw	Entre CSCFs	SIP	Utilizado 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.
Mx	CSCF o BGCF y IBCF	SIP	Utilizado por los CSCF o el BGCF y el o los IBCF para reenviarse señalización SIP de registro o control de sesión cuando va destinada a o viene de un núcleo IMS de otro operador.
Mr	S-CSCF o MRFC	SIP	Utilizado por el S-CSCF cuando necesita activar servicios de transporte.
Mp, S-T1	MRFC y MRFP (subcapa de procesado de transporte)	H.248	Utilizado por el MRFC para controlar los recursos multimedia del MRFP de acuerdo con las demandas del AS y el S-CSCF.
Mi	S-CSCF y BGCF	SIP	Utilizado por el S-CSCF cuando el S-CSCF quiere redirigir la sesión SIP a una red externa que no es NGN (RTC/RDSI o H323).
Mj	BGCF y MGCF	SIP	Utilizado por el BGCF para transferir la sesión SIP una vez ha seleccionado el MGCF (pasarela a RTC/RDSI) por el que sacar dicha sesión. En este caso, el MGCF se encuentra en el mismo dominio que el BGCF.
Mk	BGCF y MGCF (remoto)	SIP	Utilizado por el BGCF para transferir la sesión SIP una vez ha seleccionado el MGCF (pasarela a RTC/RDSI) por el que sacar dicha sesión. En este caso, el MGCF se encuentra en un dominio distinto que el BGCF.
Mg	MGCF y I-CSCFo S-CSCF	SIP	Utilizado por el MGCF para reenviar mensajes de sesiones SIP entrantes desde RTC/RDSI hacia el I-CSCF o S-CSCF.
Mn, S-T4	MGCF y T-MGF (o IMS-GW según 3GPP)	H.248	Utilizado por el MGCF para controlar los recursos en canales de voz/video del T-MGF (o IMS-MGF según 3GPP) en su conexión con la red RTC/RDSI.
Mm (3GPP)	CSCFs locales y CSCFs remotos	SIP	Utilizado para reenviar mensajes de sesiones SIP a otros servidores SIP o redes IP externas (otros dominios).
Ma, A-S7	I-CSCF y AS	SIP	Utilizado por el I-CSCF para reenviar peticiones SIP al AS con servicios públicos de identidades (PSI).
ISC, A-S4	S-CSCF y AS	SIP	Utilizado por el S-CSCF y el AS para reenviar y recibir peticiones SIP.
Cx	S-CSCF o I-CSCF y UPSF	Diameter	Utilizado por el S-CSCF y el I-CSCF para consultar al UPSF información de autenticación y autorización de usuario, perfil de suscripción, localización (S-CSCF asignado).

Nombre	Entidades que interconecta	Protocolo	Descripción
Dx	S-CSCF o I-CSCF y SLF	Diameter	Utilizado por el S-CSCF y el I-CSCF para consultar al SLF sobre la localización del UPSF que contiene la información de suscripción de un usuario.
Ib (ETSI)	IBCF y IWF	<sin especificar>	Utilizado por el IBCF para solicitar al IWF la traducción del protocolo SIP de sesión a otro protocolo.
Iw (ETSI)	IWF y otras redes IP	<sin especificar>	Utilizado por el IWF para la conversión de la señalización de sesión.
Ic, Ici	IBCF y otras redes NGN	SIP	Utilizado por el IBCF para intercomunicar dos dominios IMS. Ici (3GPP) es una especialización del Ic.
Ie (ETSI), S-T3 (ITU-T)	MGCF y SGW	<sin especificar>	Utilizado por el MGCF para intercambiar señalización SS7 sobre IP con el SGW.
Ix, S-T5 (ITU-T)	IBCF y TrGW	<sin especificar>	Utilizado por el IBCF para controlar el TrGW (p. ej. controlar las traducciones NAT).
Rc, A-S1	AS y MRB	<sin especificar>	Utilizado por el AS para solicitar recursos multimedia al MRB.
Cr (3GPP)	AS y MRFC	<sin especificar>	Utilizado por el AS para controlar los medios sin pasar por el S-CSCF
Mr' (3GPP)	AS y MRFC	SIP	Utilizado por el AS para control de sesión sin pasar por el S-CSCF.

5) Puntos de referencia de los componentes de almacenaje de información de suscripción

La siguiente tabla muestra una descripción de los puntos de referencia para el subsistema IMS, que se mencionan en los modelos de la ITU-T, la ETSI-TISPAN y el 3GPP, así como la recomendación sobre el protocolo para implementarlo.

Tabla 11. Puntos de referencia de los componentes de almacenaje de información de suscripción

Nombre	Entidades que interconecta	Protocolo	Descripción
Cx	S-CSCF o I-CSCF y UPSF	Diameter	Utilizado por el S-CSCF y el I-CSCF para consultar al UPSF información de autenticación y autorización de usuario, perfil de suscripción, localización (S-CSCF asignado).
Dx	S-CSCF o I-CSCF y SLF	Diameter	Utilizado por el S-CSCF y el I-CSCF para consultar al SLF sobre la localización del UPSF que contiene la información de suscripción de un usuario.
Sh	AS y UPSF	Diameter	Utilizado por el AF para consultar al UPSF información de autenticación y autorización de usuario, perfil de suscripción, localización (S-CSCF asignado).
Dh	AS y SLF	Diameter	Utilizado por el AF para consultar al SLF sobre la localización del UPSF que contiene la información de suscripción de un usuario.