(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 788 867**

(51) Int. CI.:

***H04W 8/12*** (2009.01)
***H04W 8/06*** (2009.01)
*H04W 76/18* (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.06.2015 PCT/EP2015/063582**

(87) Fecha y número de publicación internacional: **22.12.2016 WO16202379**

(96) Fecha de presentación y número de la solicitud europea: **17.06.2015 E 15731017 (8)**

(97) Fecha y número de publicación de la concesión europea: **18.03.2020 EP 3311602**

(54) Título: **Notificación del HSS de fallo de solicitud de conectividad para una sesión del paquete de datos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**23.10.2020**

(73) Titular/es:

**TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)**
**164 83 Stockholm, SE**

(72) Inventor/es:

**CASTELLANOS ZAMORA, DAVID y**
**HEGARTY, CORMAC**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Notificación del HSS de fallo de solicitud de conectividad para una sesión del paquete de datos

### Campo técnico

Diversas realizaciones de la invención se refieren a un nodo de control, a un nodo de servidor de abonado y a métodos y programas informáticos correspondientes. En particular, diversas realizaciones de la invención se refieren a técnicas de transmisión de un mensaje de informe en respuesta a la verificación de la autorización de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de acceso.

### Antecedentes

Las redes móviles están evolucionando actualmente de redes con conmutación de circuitos (CS, por sus siglas en inglés) pura a redes con conmutación de paquetes (PS, por sus siglas en inglés), en particular redes basadas en el Protocolo de Internet (IP, por sus siglas en inglés), y por ello se integran en infraestructuras basadas en IP que también se utilizan para Internet, la World Wide Web y la industria de la comunicación de datos.

Más específicamente, en las redes de comunicaciones móviles se han introducido tecnologías que permiten la comunicación de voz a través de una red basada en IP. Algunos ejemplos de estas redes móviles son redes móviles como las especificadas por el Proyecto de Asociación de Tercera Generación (3GPP, por sus siglas en inglés). Por ejemplo, una red de comunicaciones móviles puede implementar un Subsistema Multimedia IP (IMS, por sus siglas en inglés) tal como se especifica en la especificación técnica (TS, por sus siglas en inglés) 3GPP 23.228 (por ejemplo versión V13.2.0; 2015-) y ofrecer comunicación de voz y/o vídeo como un servicio IMS proporcionado a través de una sesión de paquetes de datos. A veces, la sesión de paquetes de datos también se designa como portadora.

Tradicionalmente, el IMS proporcionaba funcionalidad multimedia basada en IP a las redes CS. Recientemente, la funcionalidad multimedia basada en IP también se proporciona a través de redes PS. Un ejemplo consiste en el empleo del IMS para ofrecer funcionalidad de llamadas de voz y vídeo a través del sistema de Núcleo de Paquetes Evolucionado (EPC, por sus siglas en inglés) 3GPP utilizando diferentes tipos de accesos, que comprenden: los, así llamados, tipos de "acceso 3GPP" (tales como, por ejemplo, los accesos proporcionados por Evolución a Largo Plazo, LTE, por sus siglas en inglés; tecnología de acceso por radio, RAT, por sus siglas en inglés; también designada a veces como acceso 4G), así como los, así llamados, "accesos no 3GPP" (por ejemplo, accesos WiFi). Los servicios de comunicación proporcionados por los sistemas de telecomunicaciones (tipo de acceso múltiple) arriba mencionados permiten a los usuarios abonados a cualquiera de estos sistemas establecer sesiones de paquetes de datos a través de los mismos que permiten, entre otros, pero no limitados a, servicios de comunicación de voz. Por lo tanto, una expresión común utilizada por especificaciones 3GPP se denomina "Voz sobre LTE", VoLTE; aunque, como se ha comentado más arriba, el tipo de acceso utilizado por el usuario (abonado) desde su terminal para conectarse a los sistemas de telecomunicaciones puede variar (por ejemplo, tipos de acceso 3GPP y tipos de acceso no 3GPP).

El despliegue de la VoLTE requiere esfuerzos significativos de los operadores para migrar un abonado de un servicio CS heredado a un servicio VoLTE. Específicamente, un nodo de punto de acceso de la red IMS ha de ser identificado mediante una configuración correcta de un nombre de punto de acceso (APN, por sus siglas en inglés) en el terminal de un usuario asociado con un abonado que intenta acceder a una red IMS determinada para establecer la sesión de paquetes de datos correspondiente. Por ejemplo, la red IMS a la que se intenta acceder puede pertenecer al operador al que está abonado dicho usuario. La sesión de paquetes de datos se puede encaminar entonces hacia la red IMS correspondiente.

Al migrar del servicio CS heredado al servicio VoLTE, es posible que se produzca una configuración incorrecta. Por ejemplo, se pueden especificar APN incorrectos en el terminal de un abonado y/o en determinados nodos de la red de telecomunicaciones. Cuando un terminal de un abonado intenta acceder a cualquier tipo de red PS diferente al IMS surgen problemas similares.

El documento US 2015/156093 A1 describe un método en el que un UE envía una solicitud de conexión y la MME envía una solicitud de autentificación a un servidor de abonado. El servidor envía de vuelta a la MME una indicación de transmisión de error de acceso a red.

### Compendio

Existe una necesidad de técnicas que superen o mitiguen al menos algunas de las desventajas y limitaciones arriba mencionadas. En particular, existe una necesidad de técnicas que permitan detectar una configuración incorrecta con respecto a un terminal que intenta establecer la sesión de paquetes de datos, o incluso la detección de fraude.

Esta necesidad se satisface mediante las características indicadas en las reivindicaciones independientes. Las reivindicaciones dependientes definen realizaciones.

De acuerdo con un aspecto se proporciona un nodo de control de una primera red tal como se menciona en la reivindicación 1. El nodo de control comprende una primera interfaz hacia un nodo de acceso de radio de la primera

red. El nodo de control comprende además una segunda interfaz hacia un nodo de servidor de abonado. El nodo de control comprende además al menos un procesador. El al menos un procesador está configurado para recibir, a través de la primera interfaz, un mensaje de conectividad. El mensaje de conectividad incluye un identificador que indica un nodo de punto de acceso de una segunda red. El mensaje de conectividad incluye además un identificador que indica un abonado. El al menos un procesador está configurado para verificar la autorización del abonado con el fin de establecer una sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso. El al menos un procesador está configurado para enviar, a través de la interfaz, un mensaje de informe en respuesta a dicha verificación cuando ésta da como resultado una autorización fallida del abonado.

De acuerdo con un aspecto se proporciona un método tal como se menciona en la reivindicación 6. El método comprende un nodo de control de una primera red que recibe un mensaje de conectividad desde un nodo de acceso de radio de la primera red. El mensaje de conectividad incluye un identificador que indica un nodo de punto de acceso de la segunda red. El mensaje de conectividad incluye además un identificador que indica un abonado. El método comprende además verificar la autorización del abonado para establecer una sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso. El método comprende además el envío de un mensaje de informe por el nodo de control al nodo de servidor de abonado en respuesta a dicha verificación cuando ésta da como resultado una autorización fallida del abonado.

De acuerdo con otro aspecto se proporciona un nodo de servidor de abonado tal como se menciona en la reivindicación 7. El nodo de servidor de abonado comprende una interfaz hacia un nodo de control de una primera red. El nodo de servidor de abonado comprende además al menos un procesador. El al menos un procesador está configurado para recibir, a través de la interfaz, un mensaje de informe. El mensaje de informe indica una autorización fallida de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red.

De acuerdo con otro aspecto se proporciona un método tal como se menciona en la reivindicación 10. El método comprende un nodo de servidor de abonado que recibe un mensaje de informe desde un nodo de control de una primera red. El mensaje de informe indica una autorización fallida de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red.

De acuerdo con otro aspecto se proporciona un producto de programa informático que comprende código de programa para ser ejecutado por al menos un procesador de un nodo de control de una primera red, tal como se menciona en la reivindicación 11.

Se ha de entender que las características arriba mencionadas y las que aún se han de explicar más abajo pueden ser utilizadas no solo en las combinaciones respectivas indicadas, sino también en otras combinaciones o de forma aislada sin apartarse del alcance de la invención.

**Breve descripción de los dibujos**

Los anteriores efectos y características de la invención, y otros adicionales, serán evidentes a partir de la siguiente descripción detallada leída conjuntamente con los dibujos adjuntos.

La figura 1 ilustra esquemáticamente una primera red, a la que está conectado un terminal de un abonado, y una segunda red, comprendiendo la primera red una Entidad de Gestión de Movilidad que está conectada a un Servidor Local de Abonado.

La figura 2 es un diagrama de señalización que ilustra diversos aspectos de una solicitud de conectividad para una sesión de paquetes de datos de acuerdo con implementaciones de referencia.

La figura 3A es un diagrama de señalización que ilustra diversos aspectos de una solicitud de conectividad para una sesión de paquetes de datos de acuerdo con diversas realizaciones, en donde se transmite un mensaje de informe entre la Entidad de Gestión de Movilidad y el Servidor Local de Abonado, indicando el mensaje de informe la autorización fallida de un abonado para establecer la sesión de paquetes de datos.

La figura 3B es un diagrama de señalización que ilustra diversos aspectos de una solicitud de conectividad para una sesión de paquetes de datos de acuerdo con diversas realizaciones, en donde se transmite un mensaje de informe entre la Entidad de Gestión de Movilidad y el Servidor Local de Abonado, indicando el mensaje de informe la autorización otorgada a un abonado para establecer la sesión de paquetes de datos, y en donde se transmiten un mensaje de directrices y un mensaje de capacidad entre la Entidad de Gestión de Movilidad y el Servidor Local de Abonado.

La figura 4 es un diagrama de señalización que ilustra diversos aspectos de un mensaje de configuración enviado por una plataforma de servicio de acuerdo con diversas realizaciones.

La figura 5 ilustra esquemáticamente la Entidad de Gestión de Movilidad de acuerdo con diversas realizaciones.

La figura 6 ilustra esquemáticamente el Servidor Local de Abonado de acuerdo con diversas realizaciones.

La figura 7 ilustra esquemáticamente la plataforma de servicio.

La figura 8 es un diagrama de flujo que ilustra un método de acuerdo con diversas realizaciones, en el que se envía un mensaje de informe desde la Entidad de Gestión de Movilidad al Servidor Local de Abonado en respuesta a la autorización de verificación del abonado para establecer la sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso cuando dicha verificación da como resultado una autorización fallida del abonado.

La figura 9 es un diagrama de flujo que ilustra un método de acuerdo con diversas realizaciones, en el que se envía un mensaje de directrices desde el Servidor Local de Abonado a la Entidad de Gestión de Movilidad, enviándose el mensaje de informe selectivamente dependiendo de unas directrices incluidas en el mensaje de directrices.

La figura 10 es un diagrama de flujo de un método de acuerdo con diversas realizaciones, en el que el Servidor Local de Abonado recibe el mensaje de informe que indica la autorización fallida del abonado para establecer la sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso de la segunda red.

La figura 11 es un diagrama de flujo de un método de acuerdo con diversas realizaciones, en el que el Servidor Local de Abonado recibe el mensaje de informe que indica la autorización otorgada o fallida del abonado para establecer la sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso de la segunda red.

La figura 12 es un diagrama de flujo de un método de acuerdo con diversas realizaciones, en el que la plataforma de servicio recibe un mensaje de informe adicional que indica la autorización fallida del abonado para establecer la sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso de la segunda red.

**Descripción detallada de realizaciones**

A continuación, se describirán detalladamente realizaciones de la invención con referencia a los dibujos adjuntos. Se ha de entender que la siguiente descripción de realizaciones no debe ser interpretada en un sentido limitativo. El alcance de la invención no está concebido como limitado por las realizaciones descritas a continuación o por los dibujos, que se consideran solo ilustrativos.

Los dibujos deben ser considerados como representaciones esquemáticas y los elementos ilustrados en los dibujos no están mostrados necesariamente a escala. Más bien, los diversos elementos están representados de tal modo que su función y propósito general sean evidentes para un experto en la materia. Cualquier conexión o acoplamiento entre bloques funcionales, dispositivos, componentes u otras unidades físicas o funcionales que se muestran en los dibujos o se describen en la presente memoria también se puede implementar mediante una conexión o acoplamiento indirecto. También es posible establecer un acoplamiento entre componentes a través de una conexión inalámbrica. Los bloques funcionales se pueden implementar en *hardware*, *firmware*, *software* o una combinación de los mismos.

En lo sucesivo, los aspectos de verificación de la autorización de un abonado para establecer una sesión de paquetes de datos se explican principalmente en el contexto de la Tecnología de Acceso por Radio (RAT) de Evolución a Largo Plazo (LTE) 3GPP únicamente con fines ilustrativos. Se pueden aplicar fácilmente técnicas similares a diversos tipos de RAT, como Sistemas Globales para Comunicaciones Móviles (GSM, por sus siglas en inglés), Multiplexación por División de Código de Banda Ancha (WCDMA, por sus siglas en inglés), Servicio General de Radio por Paquetes (GPRS, por sus siglas en inglés), Velocidades de Transmisión de Datos Mejoradas para Evolución GSM (EDGE, por sus siglas en inglés), GPRS Mejorado (EGPRS, por sus siglas en inglés), Sistema Universal de Telecomunicaciones Móviles (UMTS, por sus siglas en inglés) y Acceso a Paquetes a Alta Velocidad (HSPA, por sus siglas en inglés).

La figura 1 ilustra esquemáticamente una arquitectura de red de comunicaciones móviles. En particular, la figura 1 ilustra esquemáticamente la arquitectura del sistema de paquetes evolucionado (EPS, por sus siglas en inglés) de la RAT LTE. El EPS comprende un núcleo de paquetes evolucionado (EPC) como red central y la Red de Acceso por Radio Terrestre de Sistema Universal de Telecomunicaciones Móviles Evolucionada (E-UTRAN, por sus siglas en inglés) para establecer un radioenlace entre un terminal 101 (UE etiquetado, equipo de usuario en la figura 1) y el EPC. El terminal puede ser cualquier tipo de dispositivo de comunicación, por ejemplo, un teléfono móvil, un ordenador portátil, un *laptop*, una pantalla de televisión inteligente, etc.

El terminal 101 está conectado a la primera red 191 que implementa el EPS y que se designa como Red Móvil Terrestre Pública Visitada (VPLMN, por sus siglas en inglés). El terminal 101 está asociado a un abonado 180. Los datos específicos de abonado del abonado se mantienen en un nodo de servidor de abonado implementado por un Servidor Local de Abonado (HSS, por sus siglas en inglés) 109 de una red designada como Red Móvil Terrestre Pública Propia (HPLMN, por sus siglas en inglés). En un escenario de itinerancia, la VPLMN 191 y la HPLMN 193 difieren entre sí. Con respecto al ejemplo ilustrado por la figura 1, se ha de tener en cuenta que algunos de los nodos ilustrados, tales como: la PGW 104, la PCRF 108, el AP 105 (así como la red IMS a la que accede el AP 105) pueden pertenecer al dominio de red de la HPLMN (193) en lugar de pertenecer al dominio de la VLPLM 191 tal como se ilustra en dicha figura.

El terminal 101 está conectado a través de un nodo 102 de acceso que implementa la E-UTRAN. Por ejemplo, el nodo 102 de acceso puede ser un nodo B evolucionado (eNB, por sus siglas en inglés). El punto 111 de referencia que implementa un radioenlace (mostrado por una línea de puntos en la figura 1) entre el terminal 101 y el nodo 102 de

acceso opera de acuerdo con el protocolo LTE-uU. Los datos de una sesión de paquetes de datos se pueden transmitir en la interfaz 111.

El nodo 102 de acceso está conectado a un nodo de pasarela implementado por una Pasarela de Servicio (SGW, por sus siglas en inglés) 103. Como tal, la SGW 103 encamina y reenvía paquetes de datos de la sesión de paquetes de datos y actúa como un ancla de movilidad del plano de usuario durante traspasos del terminal 101 entre diferentes células de la VPLMN 191. El punto 112 de referencia entre el nodo 102 de acceso y la SGW 103 funciona de acuerdo con el protocolo S1-U.

La SGW 103 está conectada, a través de un punto 113 de referencia que funciona de acuerdo con el protocolo S5, a otro nodo de pasarela implementado por una Pasarela de Red de Datos por Paquetes (PGW, por sus siglas en inglés) 104. La PGW 104 sirve como un punto de salida y punto de entrada de la VPLMN 191 para paquetes de datos de la sesión de paquetes de datos hacia una segunda red 192; en el ejemplo de la figura 1, el IMS 192 implementa la segunda red. Como tal, la PGW está conectada con un nodo 105 de punto de acceso del IMS 192 a través de un punto 114 de referencia que funciona según el protocolo SGi. El nodo 105 de punto de acceso está identificado exclusivamente por un Nombre de Punto de Acceso (APN). El APN es utilizado por el terminal 101 para intentar el establecimiento de la sesión de paquetes de datos.

La funcionalidad de directrices y carga está controlada por un nodo de control 108 implementado por una función de directrices y reglas de carga (PCRF, por sus siglas en inglés) 108. La PCRF 108 está conectada a través de un punto 118 de referencia que funciona de acuerdo con el protocolo Gx con la PGW 104.

Las funcionalidades de acceso del terminal 101 al IMS 192, por ejemplo la funcionalidad de acceso a la sesión de paquetes de datos, están controladas por un nodo de control implementado por una entidad de gestión de movilidad (MME, por sus siglas en inglés) 107. La MME 107 está conectada con el nodo 102 de acceso a través de un punto 117 de referencia que funciona de acuerdo con el protocolo S1-MME. Además, la MME 107 está conectada con la SGW 103a través de un punto 116 de referencia que funciona de acuerdo con el protocolo S11. Por ejemplo, la MME 107 verifica si el abonado 180 está autorizado para establecer la sesión de paquetes de datos accediendo al nodo 105 de punto de acceso; para ello se verifica el APN.

El HSS 109 está conectado con la MME 107 a través de un punto 119 de referencia que funciona de acuerdo con el protocolo S6a. El HSS 109 proporciona funcionalidad de gestión de abono y movilidad para el EPS. El HSS 109 almacena información de perfil de usuario utilizada para otorgar acceso selectivo al EPC. La información de perfil de usuario incluye autorización de usuario de EPS, como restricciones de acceso e itinerancia y prohibición determinada por el operador (ODB, por sus siglas en inglés). El HSS está conectado a una plataforma 141 de servicio de una red de operador 194 a través de un punto 151 de referencia propietario.

El HSS 109 también almacena información de abono con respecto a la autorización del abonado para acceder al IMS 192 a través del nodo 105 de punto de acceso. La gestión del perfil de EPS se puede lograr por medio de la información de abono. A través de la interfaz 119, la información de abono se puede proporcionar a la MME 107. La información de abono incluye, entre otras cosas, una lista de nodos de punto de acceso autorizados que se pueden identificar mediante identificadores correspondientes, implementados normalmente por APN. Es posible que la información de abono comprenda además capacidades específicas de calidad de servicio (QoS, por sus siglas en inglés) y de prioridad de asignación y retención (ARP, por sus siglas en inglés) para establecer una sesión de paquetes de datos por defecto durante la actualización de la conexión y el área de seguimiento (TA, por sus sigla en inglés).

La MME 107 recibe la información de abono de un abonado 180 dado a través del punto 190 de referencia S6a. La MME 107 tiene en cuenta la información de abono al controlar los procedimientos de movilidad específicos del abonado. En particular, la MME 107 tiene en cuenta la información de abono cuando verifica la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso. Por ejemplo, si el APN del nodo 105 de punto de acceso dado indicado por un mensaje de conectividad recibido por el nodo 102 de acceso a través del punto 111 de referencia LTE-uU desde el terminal 101 aparece como APN autorizado en la información de abono, la MME 107 puede controlar el nodo 102 de acceso y/o la SGW 103 para otorgar acceso al IMS 192 estableciendo la sesión de paquetes de datos.

A continuación se explican diversas técnicas con respecto a la notificación del resultado de dicha verificación de la autorización del abonado 180 de la MME 107 hacia el HSS 109. Aquí, el resultado puede consistir en una autorización fallida o en una autorización otorgada. También es concebible como resultado de dicha verificación una autorización de acceso limitado o una autorización temporal.

Por ejemplo, a veces la verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso da como resultado una autorización fallida del abonado 180. En este caso, la MME 107 rechaza la solicitud de conectividad correspondiente. Además, en diversos ejemplos, la MME 107 está configurada para enviar, a través del punto 119 de referencia S6a, un mensaje de informe en respuesta a dicha verificación que ha dado como resultado la autorización fallida del abonado 180. Por lo tanto, el mensaje de informe puede ser indicativo de que la verificación ha dado como resultado la autorización fallida del abonado 180. En

algunos escenarios, el mensaje de informe puede ser indicativo de que verificación ha dado como resultado el otorgamiento de la autorización del abonado 180.

A veces se pueden combinar las notificaciones de autorización fallida y autorización otorgada: en este caso, un primer mensaje de informe puede ser indicativo de una autorización fallida del abonado 180 y un segundo mensaje de informe puede ser indicativo de una autorización otorgada del abonado 180. En otros escenarios, dichos informes se pueden limitar únicamente a informes de autorización fallida o de autorización otorgada.

Por ejemplo, es posible que el mensaje de informe incluya un identificador que indique el nodo 105 de punto de acceso a través del cual el terminal 101 ha solicitado acceso al IMS 192; por ejemplo, el mensaje de informe puede incluir el APN correspondiente del nodo 105 de punto de acceso. Alternativa o adicionalmente, también es posible que el mensaje de informe incluya un identificador que indique el abonado 180; por ejemplo, el mensaje de informe puede incluir la Identidad Internacional de Abonado Móvil (IMSI, por sus siglas en inglés) y/o la Identidad Internacional de Equipo Móvil (IMEI, por sus siglas en inglés), así como el tipo de servicio solicitado. Opcionalmente, el mensaje de informe puede incluir más información. Por ejemplo, el mensaje de informe podría incluir información sobre un servicio de la sesión de paquetes de datos solicitado por el terminal 101, por ejemplo, un servicio VoLTE o similar. Al incluir información adicional en el mensaje de informe, es posible que otros nodos, como el HSS 109 y/o la plataforma 141 de servicio tomen medidas apropiadas, incluyendo la resolución de la configuración incorrecta del terminal 101 y/o la detección y prevención de fraudes. Además se puede detectar y resolver la configuración incorrecta de otros nodos que participan en el manejo de la solicitud de conectividad. Por ejemplo, se puede detectar y resolver una configuración incorrecta del nodo 102 de acceso, etc.

Con referencia a la figura 2, ahora se ilustran diversos aspectos de una verificación de autorización del abonado que solicita establecer una sesión de paquetes de datos con el IMS 192. En particular, en la figura 2 se ilustran aspectos de un escenario en el que la verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 da como resultado una autorización otorgada del abonado 180.

En el ejemplo de la figura 2 se ilustra la verificación de autorización para un escenario de servicio VoLTE que emplea el IMS 192. Sin embargo, conceptos similares se pueden aplicar fácilmente a diferentes escenarios.

En la etapa 201, el terminal 101 se conecta al EPS de la VPLMN 191 a través del nodo 102 de acceso y establece una conexión con el EPC de la VPLMN 191; como parte de la etapa 201, desde el HSS 109 se proporciona a la MME 107 la lista de APN autorizados. Para más detalles, véase 3GPP TS 23.401 V13.2.0, sección 5.3.2.

La conexión se establece utilizando una sesión de paquetes de datos por defecto. Normalmente, la sesión de paquetes de datos por defecto no implica el nodo 105 de punto de acceso del IMS 192. Esto se verifica en la etapa 202. El terminal 101 puede estar configurado de tal modo que, cuando el resultado de dicha verificación en la etapa 202 consiste en que el nodo de punto de acceso por defecto es diferente al nodo 105 de punto de acceso del IMS 192, intenta establecer la nueva sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso.

Si se requiere el establecimiento de la nueva sesión de paquetes de datos, el terminal 101 envía un mensaje 203 de conectividad. El mensaje 203 de conectividad incluye un identificador que indica el nodo 105 de punto de acceso, es decir, incluye el APN del nodo 105 de punto de acceso. Además, el mensaje 203 de conectividad incluye un identificador que indica el abonado 180, es decir, incluye la IMSI del abonado 180.

En el ejemplo de la figura 2, la MME 107 verifica en la etapa 204 la autorización del abonado 180 y otorga la autorización del abonado 180 para establecer la nueva sesión de paquetes de datos con el IMS 192. Esto se debe a que la información del abonado obtenida previamente del HSS 109 indica que el abonado 180 está autorizado para acceder al IMS 192 a través del nodo 105 de punto de acceso. El terminal 101 procede a completar el proceso de registro de IMS en la etapa 205. La nueva sesión de paquetes de datos conecta después el terminal 101 al IMS 192 a través del nodo 105 de punto de acceso.

En ocasiones se puede producir un escenario en el que la verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 da como resultado una autorización fallida del abonado 180. Se pueden concebir diversos escenarios en los que la verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 da como resultado una autorización fallida del abonado 180. Algunos ejemplos incluyen una configuración incorrecta del terminal 101 del abonado 180, fraude, un cambio en la configuración del sistema, una necesidad de suministrar nuevos servicios al abonado 180, etc.

En la figura 3A se ilustran aspectos de un escenario en el que la verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 da como resultado una autorización fallida del abonado 180. En el ejemplo de la figura 2, la verificación de autorización se ilustra para un escenario de servicio VoLTE empleando el IMS 192. Sin embargo, conceptos similares se pueden aplicar fácilmente en diferentes escenarios.

Las etapas 201 y 202, como se ilustra con respecto a la figura 2, se pueden ejecutar opcionalmente (no se muestra en la figura 3A). En este caso, el mensaje 301 de conectividad (correspondiente al mensaje 203 de conectividad) se envía desde el terminal 101 a la MME 107. Después, en la etapa 302 se verifica la autorización del abonado 180 asociado con el terminal 101.

Dicha verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 da como resultado una autorización fallida del abonado 180. Por lo tanto, la MME 107 rechaza la solicitud para establecer la sesión de paquetes de datos tal como se indica en el mensaje 203 de conectividad. El terminal 101 es informado correspondientemente por la señalización 303 de control. El registro en el IMS 192 se rechaza.

De acuerdo con algunos ejemplos, la MME 107 envía un mensaje 304 de informe en respuesta a dicha verificación que ha dado como resultado una autorización fallida del abonado 180. El mensaje 304 de informe se puede enviar a través del punto 190 de referencia S6a al HSS 109 que retiene el perfil específico del abonado que incluye información de abono.

Mediante las técnicas de envío del mensaje de informe de la MME 107 al HSS 109 es posible detectar un terminal 101 que intenta acceder a un nodo de punto de acceso no autorizado. Cuando se detecta un acceso no autorizado a un nodo de punto de acceso es posible tomar medidas correspondientes; por ejemplo, se pueden tomar medidas correctivas, contramedidas u otras medidas. En un escenario simple, el HSS 109 almacena, en la etapa 305, información del evento correspondiente para su uso posterior. Por lo tanto, el HSS 109 puede registrar internamente el evento correspondiente de la autorización fallida. La información almacenada puede incluir el identificador del nodo 105 de punto de acceso al que se ha solicitado el acceso, es decir, puede incluir el APN. La información almacenada puede incluir un identificador del abonado 180, es decir, puede incluir la IMSI.

De nuevo con referencia a la figura 3A, el HSS 109 envía opcionalmente un mensaje 306 de respuesta a la MME 107 en respuesta a la recepción del mensaje 304 de informe. Después, el HSS 109 envía un mensaje 307 de informe adicional a la plataforma 141 de servicio. En el escenario de la figura 3A, el mensaje 307 de informe adicional incluye un identificador que indica el abonado 180, es decir, que incluye la IMSI. Además, el mensaje 307 de informe adicional indica la autorización fallida del abonado 180 para establecer la sesión de paquetes de datos. Por ejemplo, esto se puede lograr incluyendo un identificador que identifique el nodo 105 de punto de acceso del IMS 192, es decir, el APN.

Por regla general, para la transmisión (envío y/o recepción) del mensaje 304 de informe y opcionalmente el mensaje 306 de respuesta se pueden utilizar diversos protocolos. Un ejemplo es la transmisión del mensaje 304 de informe y opcionalmente el mensaje 306 de respuesta como mensajes de protocolo Diameter, véase la Petición de Comentario (RFC, por sus siglas en inglés) 6733 del Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés). En particular, es posible transmitir el mensaje 305 de informe y el mensaje 306 de respuesta en el marco del procedimiento de notificación basado en Diameter definido por 3GPP TS 29.272 V13.1.0, sección 5.2.5.1.1. Es decir, el procedimiento de notificación se puede utilizar entre la MME 107 y el HSS 109 cuando el HSS 109 necesite ser notificado sobre un intento de acceso a una sesión de paquetes de datos no autorizada por la HPLMN 193. Aquí, el mensaje 305 de informe se puede designar como Petición de Notificación (NOR, por sus siglas en inglés) y el mensaje 306 de respuesta se puede designar como Respuesta de Notificación (NOA, por sus siglas en inglés).

En la figura 3B se ilustran aspectos de un escenario en el que la verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 ha dado como resultado una autorización fallida del abonado 180. En particular se ilustran aspectos de un escenario en el que, antes de enviar un mensaje 354 de informe que indica el resultado de una verificación de autorización de un abonado que intenta establecer una sesión de paquetes de datos con el IMS 192, entre la MME 107 y el HSS 109 se intercambian una capacidad de la MME 107 que envía el mensaje 354 de informe y unas directrices que solicitan a la MME 107 que ejecute selectivamente el envío del mensaje 354 de informe. Dicha ejecución selectiva del envío puede corresponder a diversos escenarios. Por ejemplo, en algunos escenarios, las directrices pueden solicitar a la MME 107 que envíe el mensaje 354 de informe por autorización fallida. Por ejemplo, en algunos escenarios, las directrices pueden solicitar a la MME 107 que no envíe el mensaje 354 de informe por autorización fallida. En algunos escenarios, las directrices pueden solicitar a la MME 107 que envíe el mensaje 354 de informe por autorización otorgada. En algunos escenarios, las directrices pueden solicitar a la MME 107 que no envíe el mensaje 354 de informe por autorización otorgada. En algunos otros escenarios, las directrices pueden solicitar a la MME 107 que envíe el mensaje 354 de informe por autorización fallida y autorización otorgada, es decir, independientemente del resultado de la verificación de autorización. En algunos escenarios, las directrices pueden solicitar a la MME 107 que envíe siempre y solo el mensaje 354 de informe por autorización fallida, y solicitar a la MME 107 que no envíe el mensaje de informe por autorización otorgada. En algunos escenarios, las directrices pueden solicitar a la MME 107 que envíe siempre y solo el mensaje 354 de informe por autorización otorgada, y puede solicitar a la MME 107 que no envíe el mensaje de informe por autorización fallida. Estos escenarios tal como se mencionan más arriba también se pueden implementar únicamente para algunos APN, es decir, dependiendo del nodo de punto de acceso particular. Por ejemplo, los escenarios arriba mencionados se pueden implementar por APN, es decir, específicamente por cada APN.

Mediante el mensaje de directrices se pueden lograr efectos favorables. En detalle, el envío del mensaje 354 de informe puede aumentar la carga de señalización global en el punto 119 de referencia S6a entre la MME 107 y el HSS 109. En ocasiones puede no ser necesario enviar el mensaje 354 de informe; luego, para evitar una carga de señalización adicional, se proporcionan técnicas que pueden solicitar selectivamente a la MME 107 que envíe el mensaje 354 de informe o solicitar a la MME 107 que no envíe el mensaje 354 de informe por medio de unas directrices. Las directrices pueden especificar bajo qué circunstancias se debe enviar el mensaje 354 de informe; esto puede incluir la especificación de los APN particulares y/o las identidades de abonado 180 y/o el resultado particular de dicha verificación de la autorización para la cual se solicita o no se solicita (o se suprime) el envío del mensaje 354 de

informe, es decir, autorización fallida u otorgada. Esto está ilustrado más abajo con respecto a los escenarios uno a ocho.

Por ejemplo, en un primer escenario, el HSS 109 implementa las directrices como una indicación de que se notificará el estado de cualquier APN autorizado, es decir, que la MME 107 enviará el mensaje de informe al HSS 109 siempre que alguno de los APN autorizados se active o inactive en la MME 107. Esto puede corresponder a notificar la autorización otorgada para todos los APN.

Por ejemplo, en un segundo escenario, el HSS 109 implementa las directrices como una indicación de que se notificará el estado de APN particulares autorizados, es decir, que la MME 107 enviará el mensaje de informe al HSS 109 siempre que uno de los APN particulares se active o inactive en la MME 107. Esto puede corresponder a notificar la autorización otorgada para un subconjunto de APN.

Por ejemplo, en un tercer escenario, el HSS 109 implementa las directrices como una indicación de que se notificará el estado de cualquier APN no autorizado, es decir, que la MME 107 enviará el mensaje de informe al HSS 109 siempre que un usuario o abonado intente establecer un conexión con cualquier APN que no esté autorizado para ese usuario o abonado. Esto puede corresponder a notificar la autorización fallida para todos los APN.

Por ejemplo, en un cuarto escenario, el HSS 109 implementa las directrices como una indicación de que se notificará el estado de APN particulares no autorizados, es decir, que la MME 107 enviará el mensaje de informe al HSS 109 siempre que un usuario o abonado intente establecer un conexión con uno de los APN particulares que no esté autorizado para ese usuario o abonado. Esto puede corresponder a notificar la autorización fallida para un subconjunto de APN.

También es posible que el HSS 109 implemente las directrices para evitar proactivamente el envío del mensaje de informe para algunos de los escenarios primero a cuarto arriba mencionados:

Por ejemplo, en un primer escenario, el HSS 109 implementa las directrices como una indicación de que el estado de cualquier APN autorizado NO será notificado, es decir, que la MME 107 NO enviará el mensaje de informe al HSS 109 siempre que cualquiera de los APN autorizados se active o inactive en la MME 107. Esto puede corresponder a NO notificar la autorización otorgada para todos los APN.

Por ejemplo, en un segundo escenario, el HSS 109 implementa las directrices como una indicación de que el estado de APN particulares autorizados NO será notificado, es decir, que la MME 107 NO enviará el mensaje de informe al HSS 109 siempre que uno de los APN particulares se active o inactive en la MME 107. Esto puede corresponder a NO notificar la autorización otorgada para un subconjunto de APN.

Por ejemplo, en un tercer escenario, el HSS 109 implementa las directrices como una indicación de que el estado de cualquier APN no autorizado NO será notificado, es decir, que la MME 107 NO enviará el mensaje de informe al HSS 109 siempre que un usuario o abonado intente establecer una conexión con cualquier APN que no esté autorizado para ese usuario o abonado. Esto puede corresponder a NO notificar una autorización fallida para todos los APN.

Por ejemplo, en un cuarto escenario, el HSS 109 implementa las directrices como una indicación de que el estado de APN particulares no autorizados NO será notificado, es decir, que la MME 107 NO enviará el mensaje de informe al HSS 109 siempre que un usuario o abonado intente establecer una conexión con uno de los APN particulares que no está autorizado para ese usuario o abonado. Esto puede corresponder a NO notificar una autorización fallida para un subconjunto de APN.

Los escenarios arriba mencionados se pueden combinar de diversas maneras. Por ejemplo, el primer y el tercer escenarios se pueden combinar. También es posible combinar el segundo y el tercer escenarios, etc. También es posible implementar las directrices de modo que se solicite el envío del mensaje de informe para algunos APN y que no se solicite/que se suprima el envío del mensaje de informe para algunos APN adicionales.

Con referencia a la figura 3B, en primer lugar se ejecuta la transmisión de un mensaje 349 de capacidad entre la MME 107 y el HSS 109. Por ejemplo, el mensaje 349 de capacidad se puede enviar desde la MME 107 al HSS 109. El mensaje 349 de capacidad puede incluir un indicador que indica una capacidad de la MME 107 para enviar el mensaje 354 de informe. Por lo tanto, en otras palabras, el mensaje 349 de capacidad puede indicar que la MME 107 puede enviar el mensaje 354 de informe en caso necesario. Alternativa o adicionalmente, también es posible que el mensaje 349 de capacidad sea enviado desde el HSS 109 a la MME 107. Aquí, el mensaje 349 de capacidad puede incluir un indicador que indica una capacidad del HSS 109 para recibir el mensaje 354 de informe. En otras palabras, es posible que las capacidades de ambos, la MME 107 y el HSS 109, se negocien. De este modo es posible asegurar la compatibilidad descendente de la operación.

A continuación, se envía un mensaje 350 de directrices desde el HSS 109 a la MME 107. El mensaje 350 de directrices incluye unas directrices. Las directrices solicitan a la MME 107 que ejecute selectivamente el envío del mensaje 354 de informe. Por ejemplo, las directrices pueden solicitar a la MME 107 que envíe siempre el mensaje 354 de informe cuando la verificación de la autorización dé como resultado una autorización fallida del abonado 180. Por ejemplo, las directrices pueden solicitar a la MME 107 que envíe siempre el mensaje 354 de informe cuando la verificación dé como

resultado una autorización otorgada del abonado 180. También es posible que las directrices soliciten a la MME 107 que envíe selectivamente el mensaje 354 de informe por cada APN. En otras palabras, es posible que las directrices diferencien entre diferentes nodos 105 de punto de acceso con respecto a dicho envío del mensaje 354 de informe. También es posible que las directrices soliciten a la MME 107 que envíe selectivamente el mensaje 354 de informe por cada IMSI. En otras palabras, es posible que las directrices diferencien entre diferentes abonados 180 con respecto a dicho envío del mensaje 354 de informe.

Generalmente, para la transmisión del mensaje 349 de capacidad y el mensaje 350 de directrices se pueden utilizar diversos protocolos. Un ejemplo consiste en la transmisión del mensaje 349 de capacidad y el mensaje 350 de directrices como mensajes de protocolo Diameter, véase IETF RFC 6733. Por ejemplo, el mensaje 349 de capacidad se puede codificar de acuerdo con el Par de Valor de Atributo (AVP, por sus siglas en inglés) de lista de características tal como se define en 3GPP TS 29.272 V13.1.0, sección 7.3.10.1 en combinación con 3GPP TS 29.229, sección 7.2. Por ejemplo, se puede definir un AVP correspondiente del tipo Agrupado. Aquí se proporciona una funcionalidad que permite descubrir y negociar capacidades específicas de los puntos finales del protocolo Diameter relevantes para el intercambio de comandos de aplicación Diameter correspondientes dentro de un punto de Referencia Diameter específico. Por ejemplo, se puede definir un AVP de lista de características que es utilizado por la MME 107 para indicar al HSS 109 que es capaz de notificar la utilización de APN autorizados en la MME 107 al HSS 109. Por ejemplo, si la MME 107 no soporta esta característica, la MME 107 no enviará el mensaje 354 de informe, por ejemplo, implementado como la NOR. Además, si el HSS 109 no soporta esta característica, la MME 107 no enviará el mensaje 354 de informe, por ejemplo, implementado como la NOR.

Por medio del mensaje 350 de directrices es posible limitar el número y tipo de mensajes 354 de informe recibidos por el HSS 109. Por ejemplo, si tanto la MME 107 como el HSS 109 soportan la transmisión del mensaje 354 de informe, el HSS 109 podría incluir como directrices en el mensaje de directrices un elemento de información que indique para qué nodos de punto de acceso particulares el HSS 109 solicita que el mensaje 354 de informe sea enviado por la MME 107. En un ejemplo, que se puede aplicar, por ejemplo, al aprovisionamiento automático de VoLTE, es posible que el HSS 109 indique que solicita el envío del mensaje 354 de informe correspondiente a todos los abonados 180 no autorizados para todos o algunos nodos 105 de punto de acceso específicos. En otro ejemplo es posible que el HSS 109 indique que solicita el envío del mensaje 354 de informe correspondiente a todos los abonados 180 no autorizados para todos o algunos nodos 105 de punto de acceso específicos, alternativa o adicionalmente. Por ejemplo, en este contexto es posible que el mensaje de informe también indique un servicio de la sesión de paquetes de datos.

Volviendo de nuevo a la figura 3B, una vez que la MME 107 ha recibido el mensaje 350 de directrices, la MME 107 recibe el mensaje 351 de conectividad correspondiente al mensaje 303 de conectividad. A continuación, la MME 107 verifica en la etapa 352 la autorización del abonado 180 asociado con el terminal 101. En el escenario de la figura 3B, la verificación da como resultado la autorización otorgada del abonado 180. Como consecuencia de ello, la MME 100 envía un mensaje 353 de control correspondiente hacia el terminal 101. Además, como las directrices incluidas en el mensaje 350 de directrices indican que para el nodo 105 de punto de acceso particular del IMS 192 se solicita positivamente el envío del mensaje 354 de informe en caso de que la verificación dé como resultado una autorización otorgada, a continuación se envía el mensaje 354 de informe de la MME 107 y éste es recibido por el HSS 109. El mensaje 354 de informe corresponde al mensaje 304 de informe, pero indica una autorización otorgada. De nuevo, el HSS 109 almacena la información correspondiente sobre el evento, en la etapa 355. Además, el HSS 356 envía el mensaje 356 de respuesta de vuelta a la MME 107. A continuación se envía un mensaje 357 de informe adicional desde el HSS 109 a la plataforma 141 de servicio. Los detalles explicados más arriba con respecto al mensaje 304 de informe y el mensaje 306 de respuesta también son aplicables al mensaje 354 de informe y al mensaje 356 de respuesta.

Como se puede ver en lo anterior, es posible informar al HSS 109 de la HPLMN 193 sobre el resultado de la verificación de autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso. La HPLMN 193 puede utilizar esta información de diversos modos, dependiendo del caso de uso.

En la figura 4 se ilustran aspectos de la HPLMN 193 que emplea el conocimiento sobre la verificación de la autorización otorgada o no del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192.

Por ejemplo, la información proporcionada por el mensaje 307, 357 de informe adicional podría ser solicitada por un nodo o entidad dados de la HPLMN 193 o una red adicional, o éstos podrían acceder a dicha información o ésta podría ser notificada a los mismos. Por ejemplo, la información podría ser proporcionada a una entidad funcional superpuesta sobre el EPC de la HPLMN 193. Por ejemplo, la información se podría almacenar en el HSS 109 y se puede acceder a la misma a petición del nodo o entidad. Alternativa o adicionalmente, la información podría ser enviada y notificada proactivamente desde el HSS 109 al nodo o entidad.

Un ejemplo de un nodo al que se podría proporcionar dicha información es la plataforma 141 de servicio. Otro ejemplo de un nodo al que se podría proporcionar dicha información es un servidor de aplicaciones del IMS 192, por ejemplo, para detección de fraude.

En la figura 4, se ilustra un escenario específico con respecto al aprovisionamiento automático de VoLTE. Aquí se confía en el envío del mensaje 401 de informe adicional a la plataforma 141 de servicio. En el escenario la figura 4, el mensaje 401 de informe adicional indica una autorización fallida del abonado 180 para establecer la sesión de paquetes de datos VoLTE con el IMS 192 a través del nodo 105 de punto de acceso. La plataforma 141 de servicios comprende un punto de decisión central en comunicación con el nodo del Sistema de Soporte de Negocios (BSS, por sus siglas en inglés) del operador. Aquí se puede tomar en última instancia la decisión de autorizar o rechazar la autorización del uso del nodo 105 de punto de acceso del IMS 192; como tal, se puede comprobar la verificación de autorización anteriormente fallida. En concreto, en la etapa 402 se verifica la autorización del abonado 180 para establecer la sesión de paquetes de datos VoLTE a través del nodo 105 de punto de acceso hacia el IMS 192. Dicha comprobación se puede basar en directrices que especifiquen cómo manejar el intento no autorizado de conexión con el nodo 105 de punto de acceso.

En un escenario en el que la plataforma 141 de servicio decide autorizar el uso del nodo 105 de punto de acceso para el servicio VoLTE, en la etapa 403 se ejecuta una solución de mitigación de aprovisionamiento. En particular se envía un mensaje de configuración al HSS 109 que actualiza la información de abono en consecuencia. Se podrían tomar medidas adicionales; por ejemplo, se pueden ejecutar actualizaciones de perfil adicionales de datos específicos del abonado si es necesario para implementar con éxito el aprovisionamiento VoLTE (no se muestra en la figura 4). A continuación, en la etapa 404, se informa al terminal 101 del abonado 180 de que el perfil ha sido actualizado. La información incluye una indicación de que ahora está disponible la VoLTE. La etapa 404 se puede basar en procedimientos de reconfiguración Por Aire (OTA, por sus siglas en inglés). Debido a ello, el mensaje 405 de conectividad se reenvía. Es decir, el terminal 101 intentar de nuevo establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso. Dado que el HSS 109 y la MME 107 se han reconfigurado en consecuencia, la verificación del abonado 180 da como resultado la autorización otorgada (véase la figura 2).

En un escenario en el que la plataforma 141 de servicio, en la etapa 402, decide negar el uso del nodo 105 de punto de acceso para el servicio VoLTE, en la etapa 406 se emplea la reconfiguración del terminal 101, por ejemplo basándose en los procedimientos de reconfiguración OTA. Aquí, una configuración errónea del terminal 101 se puede resolver a través de las medidas correctivas. Por ejemplo, el terminal 101 se puede reconfigurar para no usar el APN no autorizado. Opcionalmente se puede programar un APN diferente para el terminal 101. Un ejemplo puede estar relacionado con el empleo de un APN sensible a mayúsculas y minúsculas; aquí es posible reconfigurar el APN de la manera correcta y sensible a mayúsculas y minúsculas.

En la figura 5 se ilustra esquemáticamente la MME 107 en detalle. La MME comprende una primera interfaz 107-1 hacia el nodo 102 de acceso. La primera interfaz 107-1 se comunica a través del punto 117 de referencia S1-MME. La MME 107 comprende una segunda interfaz 107-2 hacia el HSS 109. La segunda interfaz 107-2 funciona de acuerdo con el punto 119 de referencia S6a. La MME 107 comprende además un procesador 107-3. El procesador está acoplado con una memoria 107-4 y una interfaz persona-máquina (HMI, por sus siglas en inglés) 107-5. A través de la HMI 107-5 se puede enviar información a un usuario y se puede recibir información de un usuario. La memoria 107-4 puede ser una memoria no volátil. El código del programa se puede almacenar en la memoria 107-4. El procesador 107-3 puede estar configurado para ejecutar el código del programa. La ejecución del código de programa por el procesador 107-3 puede hacer que el procesador ejecute técnicas tal como se ilustra en la presente memoria con respecto al envío del mensaje 304, 354 de informe, la recepción del mensaje 350 de directrices, el envío del mensaje 349 de capacidad, la recepción del mensaje 349 de capacidad, la verificación de la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso, etc.

En la figura 6 se ilustra esquemáticamente el HSS 109 en detalle. El HSS 109 comprende una primera interfaz 109-1 hacia la MME 107. La primera interfaz 109-1 funciona de acuerdo con el punto 119 de referencia S6a. Además, el HSS 109 comprende una segunda interfaz 109-2 hacia la plataforma 141 de servicio. Además, el HSS 109 comprende un procesador 109-3. El procesador 109-3 está acoplado con una memoria 109-4 y una HMI 109-5. A través de la HMI 109-5 se puede enviar información a un usuario y recibir información de un usuario. La memoria 109-4 puede ser una memoria no volátil. Por ejemplo, el código del programa se puede almacenar en la memoria 109-4 y puede ser ejecutado por el procesador 109-3. La ejecución del código de programa por el procesador 109-3 hace que el procesador ejecute técnicas tal como se ilustra en la presente memoria con respecto a la recepción del mensaje 304, 354 de informe, el envío y/o la recepción del mensaje 349 de capacidad, la creación de las directrices y el envío del mensaje 350 de directrices, el envío del mensaje 307, 357 de informe adicional, etc.

En la figura 7 se ilustra esquemáticamente la plataforma 141 de servicio en detalle. La plataforma 141 de servicio comprende una primera interfaz 141-1 hacia el HSS 109. La plataforma 141 de servicio comprende una segunda interfaz 141-2 hacia el terminal 101; aquí se pueden realizar procedimientos OTA por medio de comunicaciones 152 al terminal a través de los nodos de acceso correspondientes. Opcionalmente, la plataforma 141 de servicio puede comprender otras interfaces, por ejemplo una interfaz para un servidor de aplicaciones del IMS 192. En el ejemplo de la figura 7, la plataforma 141 de servicio comprende tres entidades 141A, 141B, 141C: un nodo 141A de punto de decisión que toma la decisión de otorgar o denegar el acceso del abonado al IMS 192, es decir, verifica la autorización. Un nodo 141B de mediación de aprovisionamiento que controla la comunicación con el terminal 101, por ejemplo implementa la configuración OTA. Un nodo de BSS 141C que implementa la funcionalidad de control y gestión. Cada una de las tres entidades 141A, 141B, 141C comprende un procesador 141-3, 141-6, 141-9, una memoria 141-4, 141-7, 141-10 y una HMI 141-5, 141-8, 141-11. Por ejemplo, las memorias 141-4, 141-7, 141-10 pueden ser memorias no

volátiles y pueden almacenar un código de programa que, cuando es ejecutado por los procesadores 141-3, 141-6, 141-9 respectivos, provoca la ejecución de las técnicas ilustradas aquí con respecto al aprovisionamiento automático de VoLTE, etc. También es posible que las tres entidades 141A, 141 B, 141 C se implementen como *software* en un solo dispositivo físico.

La figura 8 es un diagrama de flujo de un método de acuerdo con diversas realizaciones. Por ejemplo, el método como se ilustra en la figura 8 puede ser ejecutado por el procesador 107-3 de la MME 107. En la etapa 801 se recibe el mensaje 203, 301, 405 de conectividad desde el nodo 102 de acceso. En la etapa 802 se verifica la autorización del abonado 180 para establecer una sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso del IMS 192. Si la verificación de autorización de la etapa 802 da como resultado una autorización fallida, en la etapa 803, se envía el mensaje 304, 354 de informe al HSS 109. En el ejemplo de la figura 8 no es necesario tener en cuenta unas directrices antes de enviar el mensaje 304, 354 de informe en la etapa 803; por ejemplo, el mensaje 803 de informe siempre se puede enviar cuando la verificación 802 da como resultado una autorización fallida.

La figura 9 es un diagrama de flujo de un método de acuerdo con diversas realizaciones. Aquí se tienen en cuenta unas directrices antes de enviar el mensaje de informe. Por ejemplo, el procesador 107-3 de la MME 107 puede ejecutar el método como se ilustra en la figura 9. En la etapa 901, la MME 107 recibe desde el HSS 109 el mensaje 350 de directrices que incluye las directrices. Las directrices solicitan que el HSS 107 ejecute selectivamente el envío del mensaje 304, 354 de informe.

Opcionalmente se puede enviar y/o recibir el mensaje 349 de capacidad. El mensaje 349 de capacidad incluye un indicador que indica la capacidad del HSS 109 y/o del MEE 107 para recibir/enviar el mensaje 304, 354 de informe.

A continuación se recibe el mensaje 203, 301, 405 de conectividad. En la etapa 903 se verifica la autorización del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso del IMS 192. Si la verificación 903 de autorización da como resultado una autorización fallida, en la etapa 904 se verifica si las directrices requieren el envío del mensaje 304, 354 de informe. En este sentido, en la etapa 904 se puede verificar si la información específica del nodo de punto de acceso está incluida en las directrices. Además, en la etapa 904 se puede verificar si para el caso de autorización fallida se requiere el envío del mensaje 304, 354 de informe, por ejemplo para el nodo 105 de punto de acceso específico según lo indicado por el APN incluido en el mensaje 203, 301, 405 de conectividad recibido en la etapa 902. Si dicha verificación en la etapa 904 da como resultado que las directrices requieren el envío del mensaje de informe, en la etapa 906 se envía el mensaje 304, 354 de informe; aquí se puede verificar opcionalmente si el HSS 109 es capaz de recibir el mensaje 304, 354 de informe.

Si la verificación 903 de autorización da como resultado una autorización otorgada, en la etapa 905 se comprueba si las directrices requieren el envío del mensaje 304, 354 de informe. A este respecto, en la etapa 905 se puede verificar si la información específica del nodo de punto de acceso está incluida en las directrices. Además, en la etapa 905 se puede verificar si para el caso de autorización otorgada se requiere el envío del mensaje 304, 355 de informe, por ejemplo para el nodo 105 de punto de acceso específico según lo indicado por el APN incluido en el mensaje 203, 301, 405 de conectividad recibido en la etapa 902. Si dicha verificación en la etapa 905 da como resultado que las directrices requieren el envío del mensaje de informe, en la etapa 906 se envía el mensaje 304, 354 de informe.

Como se comprenderá a partir de las figuras 8 y 9, el envío del mensaje 304, 354 de informe tiene lugar en respuesta a dicha verificación que da como resultado una autorización fallida y/u otorgada. Como tal, el mensaje 304, 354 de informe indica una autorización fallida y/u otorgada. Por ejemplo, el mensaje 304, 354 de informe puede incluir un indicador que indica el resultado de la verificación de autorización. También es posible que el resultado de la verificación de autorización esté indicado implícitamente en el mensaje 304, 354 de informe.

La figura 10 es un diagrama de flujo de un método de acuerdo con diversas realizaciones. Por ejemplo, el método puede ser ejecutado por el procesador 109-3 del HSS 109. En la etapa 1001 se recibe el mensaje 304, 354 de informe. El mensaje 304, 354 de informe indica una autorización fallida del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso del IMS 192.

La figura 11 es un diagrama de flujo de un método de acuerdo con diversas realizaciones. Por ejemplo, el método puede ser ejecutado por el procesador 109-3 del HSS 109. En la etapa 1101, el HSS 109 envía el mensaje 350 de directrices que incluye las directrices. En la etapa 1101, el HSS 109 recibe el mensaje 304, 354 de informe. Dependiendo de las directrices, el mensaje 304, 354 de informe puede indicar una autorización fallida y/u otorgada del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso.

Opcionalmente, en los métodos ilustrados en las figuras 10 y 11 es posible crear unas directrices y enviar el mensaje 350 de directrices al HSS 107. Opcionalmente, en los métodos ilustrados en las figuras 10 y 11 es posible enviar un mensaje de capacidad que incluye un indicador que indica la capacidad del HSS 109 para recibir el mensaje 304, 354 de informe.

La figura 12 es un diagrama de flujo de un método de acuerdo con diversas realizaciones. Por ejemplo, el método puede ser ejecutado por al menos algunos de los procesadores 141-3, 141-6, 141-9 de la plataforma 141 de servicio. En la etapa 1201 se recibe el mensaje 357, 401 de informe adicional. El mensaje 357, 401 de informe adicional indica

una autorización fallida del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso del IMS 192. Por ejemplo, el mensaje 357, 401 de informe adicional puede incluir un identificador que indica el nodo 105 de punto de acceso, es decir, el APN. Por ejemplo, el mensaje 357, 401 de informe adicional puede incluir un identificador que indica el abonado 180, es decir, la IMSI.

A continuación, se verifica la autorización fallida del abonado 180 para establecer la sesión de paquetes de datos con el IMS 192 a través del nodo 105 de punto de acceso del IMS 192. En respuesta a dicha verificación se envía el mensaje 404, 406 de configuración, por ejemplo al HSS 109 y/o al terminal 101. El contenido del mensaje 404, 406 de configuración y/o el destinatario del mensaje 404, 406 de configuración pueden depender del resultado de dicha verificación de la autorización. Por ejemplo, el mensaje 404, 406 de configuración se puede utilizar para reconfigurar el terminal 101 mediante procedimientos OTA. También es posible que mediante el mensaje 404, 406 de configuración se reconfiguren determinados parámetros del HSS 109. También es posible que mediante el mensaje de configuración 404, 406 se señale una detección de fraude al IMS 192.

Más arriba se han explicado diversos aspectos y realizaciones con referencia al IMS 192 como un ejemplo de una red PS. Sin embargo, también es posible aplicar fácilmente técnicas correspondientes a diferentes clases y tipos de redes PS.

Además se han explicado diversos aspectos y realizaciones con referencia al caso de uso del servicio VoLTE. Sin embargo, también es posible aplicar fácilmente técnicas correspondientes a diferentes clases y tipos de servicios de la sesión de paquetes de datos.

Además, más arriba se han explicado diversos aspectos y realizaciones con referencia a la MME 107 y al HSS 109. Sin embargo, también es posible aplicar fácilmente técnicas correspondientes a diferentes clases y tipos de nodos de control y nodos de servidor de abonado. Por ejemplo, en lugar de depender de la RAT LTE 3GPP, es posible implementar técnicas correspondientes para la red central del Servicio General de Radio por Paquetes (GPRS) para otras RAT. Por ejemplo, con referencia a las figuras 3A, 3B y la figura 4, en lugar de la MME 107, la funcionalidad correspondiente se puede implementar con respecto a un Nodo de Soporte GPRS de Servicio (SGSN, por sus siglas en inglés) en conexión con la Red de Acceso por Radio Terrestre UMTS (UTRAN), a veces designada como tecnología "3G". Por ejemplo, con referencia a las figuras 3A, 3B y la figura 4, en lugar de la MME 107, la funcionalidad correspondiente se puede implementar con respecto a una entidad de Autentificación, Autorización y Contabilidad (AAA, por sus siglas en inglés) en combinación con la RAT de Red de Área Local Inalámbrica (WLAN, por sus siglas en inglés, o Wi-Fi), véanse los estándares del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por su siglas en inglés) de la familia 802.11. El SGSN y la AAA pueden estar configurados para interactuar con el HSS 109 del mismo modo que el ilustrado más arriba con respecto a la MME 107, y en particular tal como se ilustra con referencia a las figuras 3A, 3B y 4. Se hace referencia a 3GPP TS 29.272 y 3GPP TS 23.401, donde se define el punto S6d de referencia entre el SGSN y el HSS 109. Se hace referencia adicional a 3GPP TS 29.273 y 3GPP TS 23.402, donde se define el punto SWx de referencia entre la AAA y el HSS 109.

En resumen, más arriba se han ilustrado técnicas que permiten notificar el resultado de la verificación de la autorización de un abonado para establecer una sesión de paquetes de datos con una PDN. El operador puede utilizar dicha información en diversos casos de uso. Un ejemplo es el aprovisionamiento automático de VoLTE. Otro ejemplo es la detección de fraude. Otro ejemplo más es la detección de una configuración incorrecta del terminal. Se han dado ejemplos en los que el envío de un mensaje de informe correspondiente se ejecuta selectivamente en función de unas directrices. Es posible configurar las directrices bajo demanda. Para ello, el mensaje de directrices se puede enviar al nodo de control que envía el mensaje de informe. El mensaje de directrices puede incluir las directrices. De este modo se puede limitar la carga de señalización.

En resumen, como se ha explicado más arriba, dependiendo de las directrices, el nodo de servidor de abonado puede solicitar al nodo de control que ejecute selectivamente dicho envío del mensaje de informe, por ejemplo en función del resultado de dicha verificación de autorización:

Por consiguiente, de acuerdo con diversas realizaciones, un nodo de servidor de abonado puede comprender una interfaz hacia un nodo de control de una primera red; y al menos un procesador configurado para enviar, a través de la interfaz, un mensaje de directrices que incluye unas directrices. El al menos un procesador puede estar configurado para recibir, a través de la interfaz, un mensaje de informe que indica una autorización fallida del abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe.

Por consiguiente, de acuerdo con diversas realizaciones, un nodo de servidor de abonado puede comprender una interfaz hacia un nodo de control de una primera red; y al menos un procesador configurado para enviar, a través de la interfaz, un mensaje de directrices que incluye unas directrices. El al menos un procesador puede estar configurado para recibir, a través de la interfaz, un mensaje de informe que indica una autorización otorgada del abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe.

Por consiguiente, de acuerdo con diversas realizaciones, un método puede comprender un nodo de servidor de abonado que envía, a un nodo de control de una primera red, un mensaje de directrices que incluye unas directrices; y el nodo de servidor de abonado que recibe, desde el nodo de control, un mensaje de informe que indica una autorización fallida de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe.

Por consiguiente, de acuerdo con diversas realizaciones, un método puede comprender un nodo de servidor de abonado que envía, a un nodo de control de una primera red, un mensaje de directrices que incluye unas directrices; y el nodo de servidor de abonado que recibe, desde el nodo de control, un mensaje de informe que indica una autorización otorgada de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe.

Por consiguiente, de acuerdo con diversas realizaciones, un producto de programa informático puede comprender un código de programa que ha de ser ejecutado por al menos un procesador de un nodo de servidor de abonado, en donde la ejecución del código del programa hace que el al menos un procesador ejecute un método en el que el nodo de servidor de abonado envía a un nodo de control de una primera red un mensaje de directrices que incluye unas directrices; y el nodo de servidor de abonado recibe, desde el nodo de control, un mensaje de informe que indica una autorización fallida de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe.

Por consiguiente, de acuerdo con diversas realizaciones, un producto de programa informático puede comprender un código de programa que ha de ser ejecutado por al menos un procesador de un nodo de servidor de abonado, en donde la ejecución del código del programa hace que el al menos un procesador ejecute un método en el que el nodo de servidor de abonado envía a un nodo de control de una primera red un mensaje de directrices que incluye unas directrices; y el nodo de servidor de abonado recibe, desde el nodo de control, un mensaje de informe que indica una autorización otorgada de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe.

Por consiguiente, de acuerdo con diversas realizaciones se proporciona un sistema. El sistema puede comprender un nodo de servidor de abonado y un nodo de control de una primera red. El nodo de servidor de abonado puede comprender una interfaz hacia el nodo de control de la primera red. El nodo de servidor de abonado puede comprender además al menos un procesador. El al menos un procesador del nodo de servidor de abonado puede estar configurado para enviar, a través de la interfaz, un mensaje de directrices que incluye unas directrices. El al menos un procesador del nodo de servidor de abonado puede estar configurado para recibir, a través de la interfaz, un mensaje de informe. El mensaje de informe puede indicar una autorización fallida de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe. El nodo de control puede comprender una primera interfaz hacia un nodo de acceso de radio de la primera red. El nodo de control puede comprender además una segunda interfaz hacia el nodo de servidor de abonado. El nodo de control puede comprender además al menos un procesador configurado para recibir, a través de la segunda interfaz, el mensaje de directrices. El al menos un procesador del nodo de control puede estar configurado para recibir, a través de la primera interfaz, un mensaje de conectividad. El mensaje de conectividad puede incluir un identificador que indica el nodo de punto de acceso de la segunda red y además puede incluir un identificador que indica el abonado. El al menos un procesador del nodo de control puede estar configurado para verificar la autorización del abonado para establecer la sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso. El al menos un procesador del nodo de control puede estar configurado para enviar, a través de la segunda interfaz, el mensaje de informe en respuesta a dicha verificación. El al menos un procesador del nodo de control puede estar configurado para ejecutar selectivamente dicho envío del mensaje de informe en función de las directrices.

Por consiguiente, de acuerdo con diversas realizaciones se proporciona un sistema. El sistema puede comprender un nodo de servidor de abonado y un nodo de control de una primera red. El nodo de servidor de abonado puede comprender una interfaz hacia el nodo de control de la primera red. El nodo de servidor de abonado puede comprender además al menos un procesador. El al menos un procesador del nodo de servidor de abonado puede estar configurado para enviar, a través de la interfaz, un mensaje de directrices que incluye unas directrices. El al menos un procesador del nodo de servidor de abonado puede estar configurado para recibir, a través de la interfaz, un mensaje de informe. El mensaje de informe puede indicar una autorización otorgada de un abonado para establecer una sesión de paquetes de datos con una segunda red a través de un nodo de punto de acceso de la segunda red. Las directrices pueden solicitar al nodo de control que ejecute selectivamente el envío del mensaje de informe. El nodo de control puede comprender una primera interfaz hacia un nodo de acceso de radio de la primera red. El nodo de control puede comprender además una segunda interfaz hacia el nodo de servidor de abonado. El nodo de control puede comprender además al menos un procesador configurado para recibir, a través de la segunda interfaz, el mensaje de directrices. El al menos un procesador del nodo de control puede estar configurado para recibir, a través de la primera interfaz, un mensaje de conectividad. El mensaje de conectividad puede incluir un identificador que indica el nodo de punto de

acceso de la segunda red y además puede incluir un identificador que indica el abonado. El al menos un procesador del nodo de control puede estar configurado para verificar la autorización del abonado para establecer la sesión de paquetes de datos con la segunda red a través del nodo de punto de acceso. El al menos un procesador del nodo de control puede estar configurado para enviar, a través de la segunda interfaz, el mensaje de informe en respuesta a dicha verificación. El al menos un procesador del nodo de control puede estar configurado para ejecutar selectivamente dicho envío del mensaje de informe en función de las directrices.

Aunque la invención se ha mostrado y descrito con respecto a determinadas realizaciones preferidas, a otros expertos en la materia se les ocurrirán modificaciones después de leer y comprender la especificación. La presente invención incluye todas estas modificaciones y está limitada únicamente por el alcance de las reivindicaciones adjuntas.

**REIVINDICACIONES**

1. Un nodo (107) de control de una primera red (191), que comprende:

- una primera interfaz (107-1) hacia un nodo (102) de acceso de radio de la primera red (191),

- una segunda interfaz (107-2) hacia un nodo (109) de servidor de abonado,

- al menos un procesador (107-3) configurado para recibir, a través de la segunda interfaz (107-1), un mensaje (203, 301, 405, 1301) de conectividad, incluyendo el mensaje (203, 301, 405, 1301) de conectividad un identificador que indica un nodo (105) de punto de acceso de una segunda red (192) y además un identificador que indica un abonado (180),

en donde el al menos un procesador (107-3) está configurado para verificar la autorización del abonado (180) para establecer una sesión de paquetes de datos con la segunda red (192) a través del nodo (105) de punto de acceso,

en donde el al menos un procesador (107-3) está configurado para enviar, a través de la segunda interfaz (107-2), un mensaje (304, 354, 1304) de informe en respuesta a dicha verificación que ha dado como resultado una autorización fallida del abonado (180),

en donde el al menos un procesador (107-3) está configurado para recibir, a través de la segunda interfaz (107-2), un mensaje (350) de directrices que incluye unas directrices, incluyendo las directrices un identificador que indica al menos un nodo (105) de punto de acceso candidato para el que se solicita dicho envío del mensaje (304, 354, 1304) de informe, en donde el al menos un procesador (107-3) está configurado para ejecutar selectivamente dicho envío del mensaje (304, 354, 1304) de informe dependiendo de si el mensaje de conectividad identifica uno de los nodos de punto de acceso candidato.

2. El nodo (107) de control de una cualquiera de las reivindicaciones precedentes,

en donde el mensaje (304, 354, 1304) de informe incluye un identificador que indica el nodo (105) de punto de acceso.

3. El nodo de control (107) de la reivindicación 1,

en donde el mensaje (304, 354, 1304) de informe incluye un identificador que indica el abonado (180).

4. El nodo (107) de control de una cualquiera de las reivindicaciones precedentes,

en donde el al menos un procesador (107-3) está configurado para enviar, a través de la segunda interfaz (107-2), un mensaje (349) de capacidad que incluye un indicador que indica una capacidad del nodo (107) de control para enviar el mensaje (304, 354, 1304) de informe.

5. El nodo (107) de control de una cualquiera de las reivindicaciones precedentes,

en donde el nodo (107) de control se selecciona entre el grupo que comprende: una Entidad de Gestión de Movilidad, MME, por sus siglas en inglés; un Nodo de Soporte de Servicio General de Radio por Paquetes, SGSN, por sus siglas en ingles; un nodo de Autentificación, Autorización y Contabilidad, AAA, por sus siglas en inglés.

6. Un método realizado mediante:

- un nodo (107) de control de una primera red (191), comprendiendo el método:

- la recepción, desde un nodo (102) de acceso de radio de la primera red (191), de un mensaje (203, 301, 405, 1301) de conectividad, incluyendo el mensaje (203, 301, 405, 1301) de conectividad un identificador que indica un nodo (105) de punto de acceso de una segunda red (192) y también un identificador que indica un abonado (180),

- la verificación de la autorización del abonado (180) para establecer una sesión de paquetes de datos con la segunda red (192) a través del nodo (105) de punto de acceso,

- en respuesta a dicha verificación cuando ésta da como resultado una autorización fallida del abonado (180): el envío, por parte del nodo (107) de control, de un mensaje (304, 354, 1304) de informe a un nodo (109) de servidor de abonado,

- la recepción, por parte del nodo (107) de control, de un mensaje (350) de directrices que incluye unas directrices desde el nodo (109) de servidor de abonado, incluyendo las directrices un identificador que indica al menos un nodo (105) de punto de acceso candidato para el que se solicita dicho envío del mensaje (304, 354, 1304) de informe,

en donde dicho envío del mensaje (304, 354, 1304) de informe se ejecuta selectivamente en función de si el mensaje de conectividad identifica uno de los puntos de acceso candidatos.

7. Un nodo (109) de servidor de abonado que comprende:

- una interfaz (109-1) hacia un nodo (107) de control de una primera red (191),

- al menos un procesador (109-3) configurado para enviar, a través de la interfaz (109-1), un mensaje (350) de directrices que incluye unas directrices,

en donde las directrices incluyen un identificador que indica al menos un nodo (105) de punto de acceso candidato para el que se solicita el envío de un mensaje (304, 354, 1304) de informe,

en donde el al menos un procesador (109-3) está configurado para recibir, a través de la interfaz (109-1), un mensaje (304, 354, 1304) de informe que indica una autorización fallida de un abonado (180) para establecer una sesión de paquetes de datos con una segunda red (192) a través de un nodo (105) de punto de acceso de la segunda red (192),

cuando el nombre del punto de acceso de la segunda red (192) identifica uno de los puntos de acceso candidatos.

8. El nodo (109) de servidor de abonado de la reivindicación 7,

en donde la sesión de paquetes de datos es una sesión de paquetes de datos de llamada de voz, en donde el nodo de servidor de abonado comprende

- al menos una interfaz (109-2) adicional hacia una plataforma (141) de suministro de servicio para gestionar la autorización específica de abonado de la sesión de paquetes de datos de llamada de voz,

en donde el al menos un procesador (109-3) está configurado para enviar, a través de la al menos una interfaz (109-2) adicional, un mensaje (307, 401) de informe adicional, incluyendo el mensaje (307, 401) de informe adicional un identificador que indica el abonado (180), indicando el mensaje (307, 401) de informe adicional además una autorización fallida del abonado (180) para establecer la sesión de paquetes de datos de llamada de voz.

9. El nodo (109) de servidor de abonado de las reivindicaciones 7 u 8, que además comprende

- al menos una interfaz (109-2) adicional hacia un nodo de servidor de aplicaciones de la segunda red (192),

en donde el al menos un procesador (109-3) está configurado para enviar, a través de la al menos una interfaz (109-2) adicional, un mensaje (307, 401) de informe adicional, incluyendo el mensaje (307, 401) de informe adicional un identificador que indica el abonado (180), indicando el mensaje (307, 401) de informe adicional además una autorización fallida del abonado (180) para establecer la sesión de paquetes de datos de llamada de voz.

10. Un método realizado mediante:

- un nodo (109) de servidor de abonado, comprendiendo el método:

- el envío, a un nodo (107) de control de una primera red (191), de un mensaje (350) de directrices que incluye unas directrices, en donde las directrices incluyen un identificador que indica al menos un nodo (105) de punto de acceso candidato para el que se solicita el envío del mensaje (304, 354, 1304) de informe,

- la recepción por el nodo (109) de servidor de abonado, desde el nodo (107) de control, de un mensaje (304, 354, 1304) de informe que indica una autorización fallida de un abonado (180) para establecer una sesión de paquetes de datos con una segunda red (192) a través de un nodo (105) de punto de acceso de la segunda red (192),

cuando el nombre del punto de acceso de la segunda red identifica uno de los puntos de acceso candidatos.

11. Un producto de programa informático que comprende un código de programa que ha de ser ejecutado por al menos un procesador de un nodo (107) de control de una primera red (191) o de un nodo de servidor de abonado, en donde la ejecución del código de programa hace que el al menos un procesador ejecute un método tal como se menciona en cualquiera de las reivindicaciones 6 y 10, respectivamente.

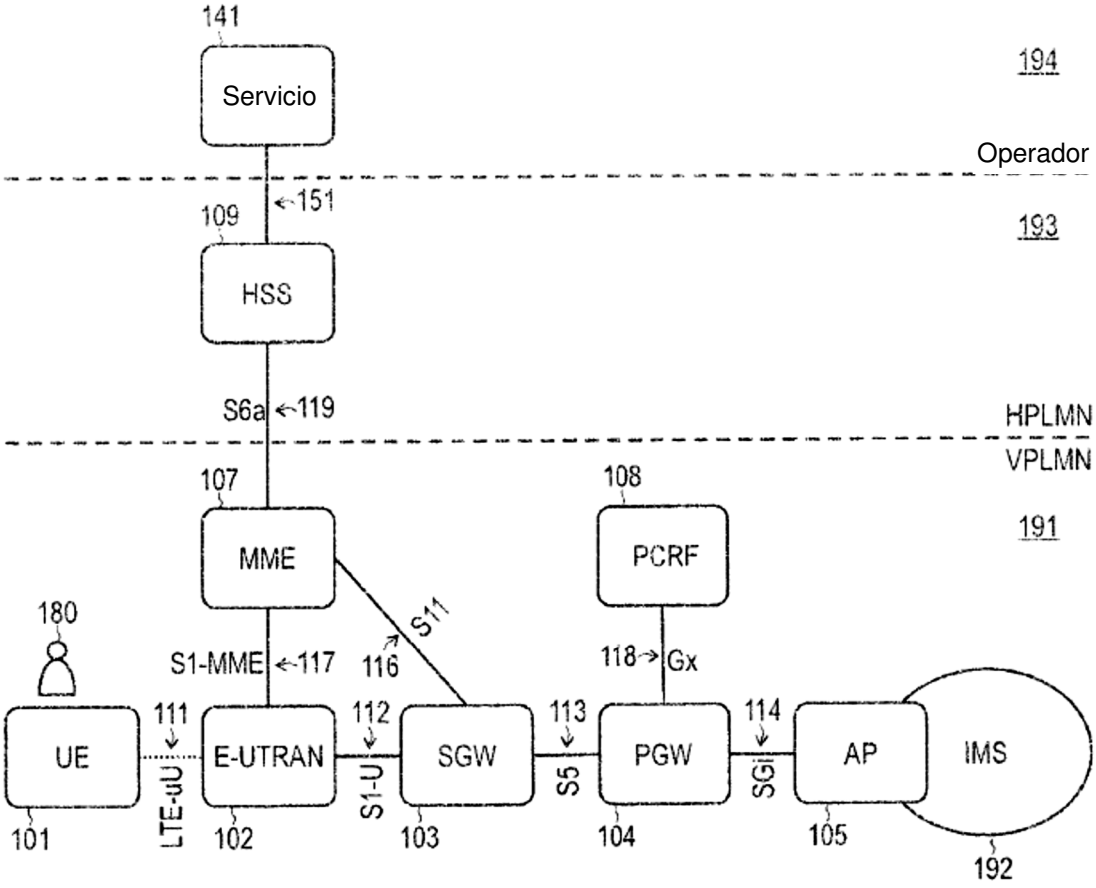
141
Servicio
194
Operador
151
109
193
HSS
S6a
119
HPLMN
VPLMN
107
108
191
MME
PCRF
180
S11
S1-MME
117
116
118
Gx
111
112
113
114
UE
E-UTRAN
SGW
PGW
AP
IMS
LTE-uU
S1-U
S5
SGi
101
102
103
104
105
192

Fig. 1

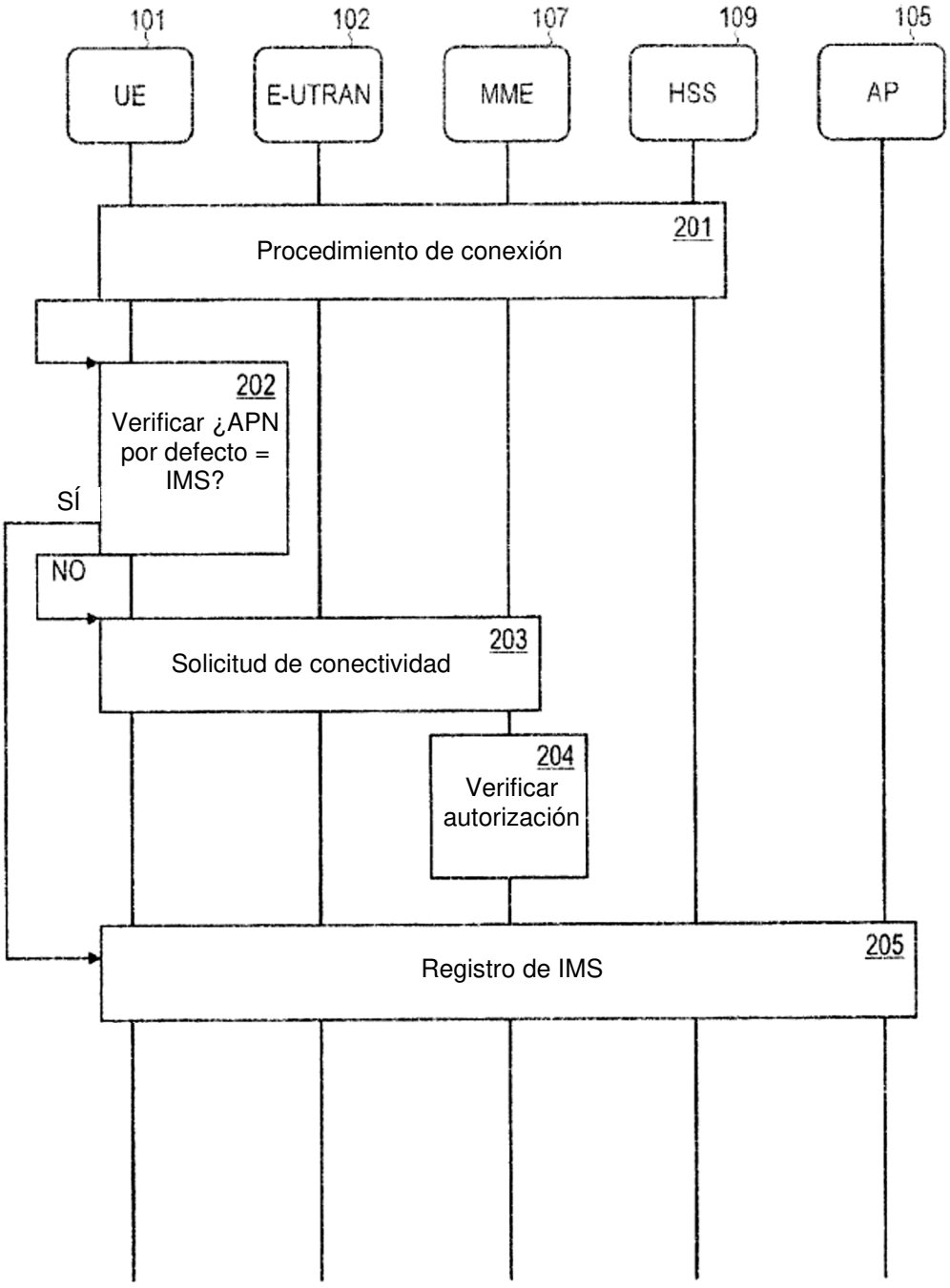
101
102
107
109
105
UE
E-UTRAN
MME
HSS
AP
201
Procedimiento de conexión
202
Verificar ¿APN por defecto = IMS?
SÍ
NO
203
Solicitud de conectividad
204
Verificar autorización
205
Registro de IMS

Fig. 2

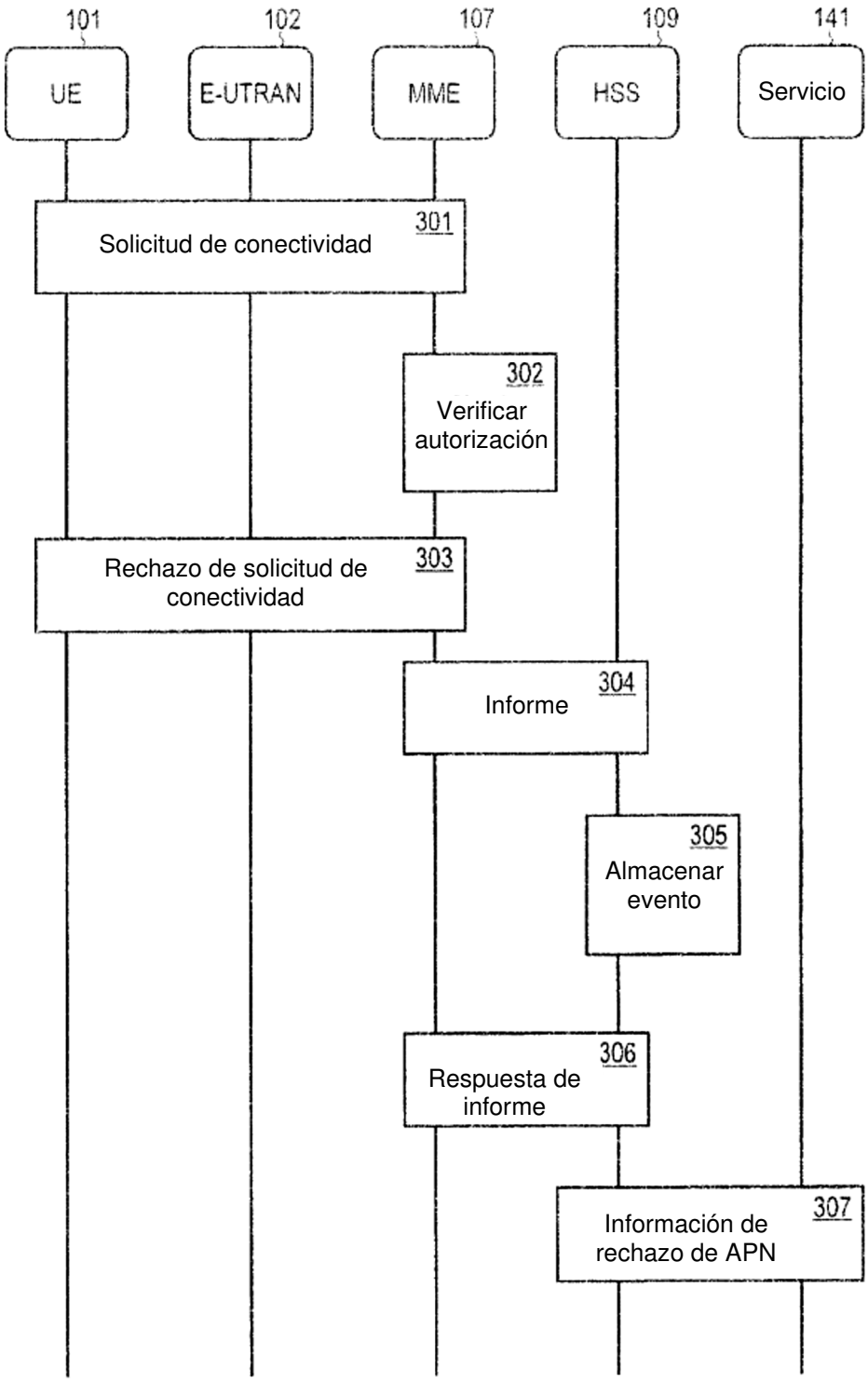
101
102
107
109
141
UE
E-UTRAN
MME
HSS
Servicio
Solicitud de conectividad
301
302
Verificar autorización
Rechazo de solicitud de conectividad
303
Informe
304
305
Almacenar evento
306
Respuesta de informe
307
Información de rechazo de APN

Fig. 3A

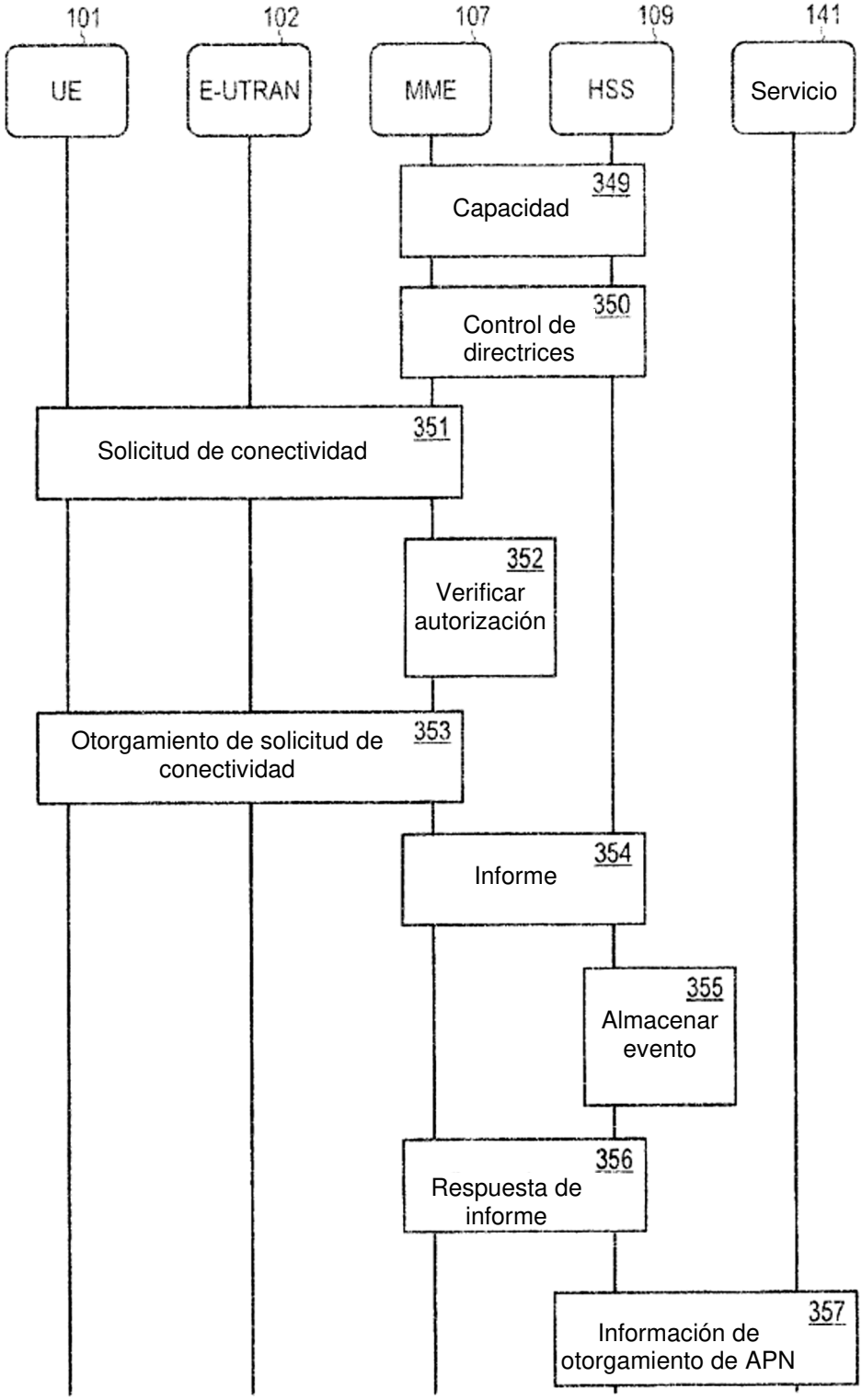
101
UE
102
E-UTRAN
107
MME
109
HSS
141
Servicio
349
Capacidad
350
Control de directrices
351
Solicitud de conectividad
352
Verificar autorización
353
Otorgamiento de solicitud de conectividad
354
Informe
355
Almacenar evento
356
Respuesta de informe
357
Información de otorgamiento de APN

Fig. 3B

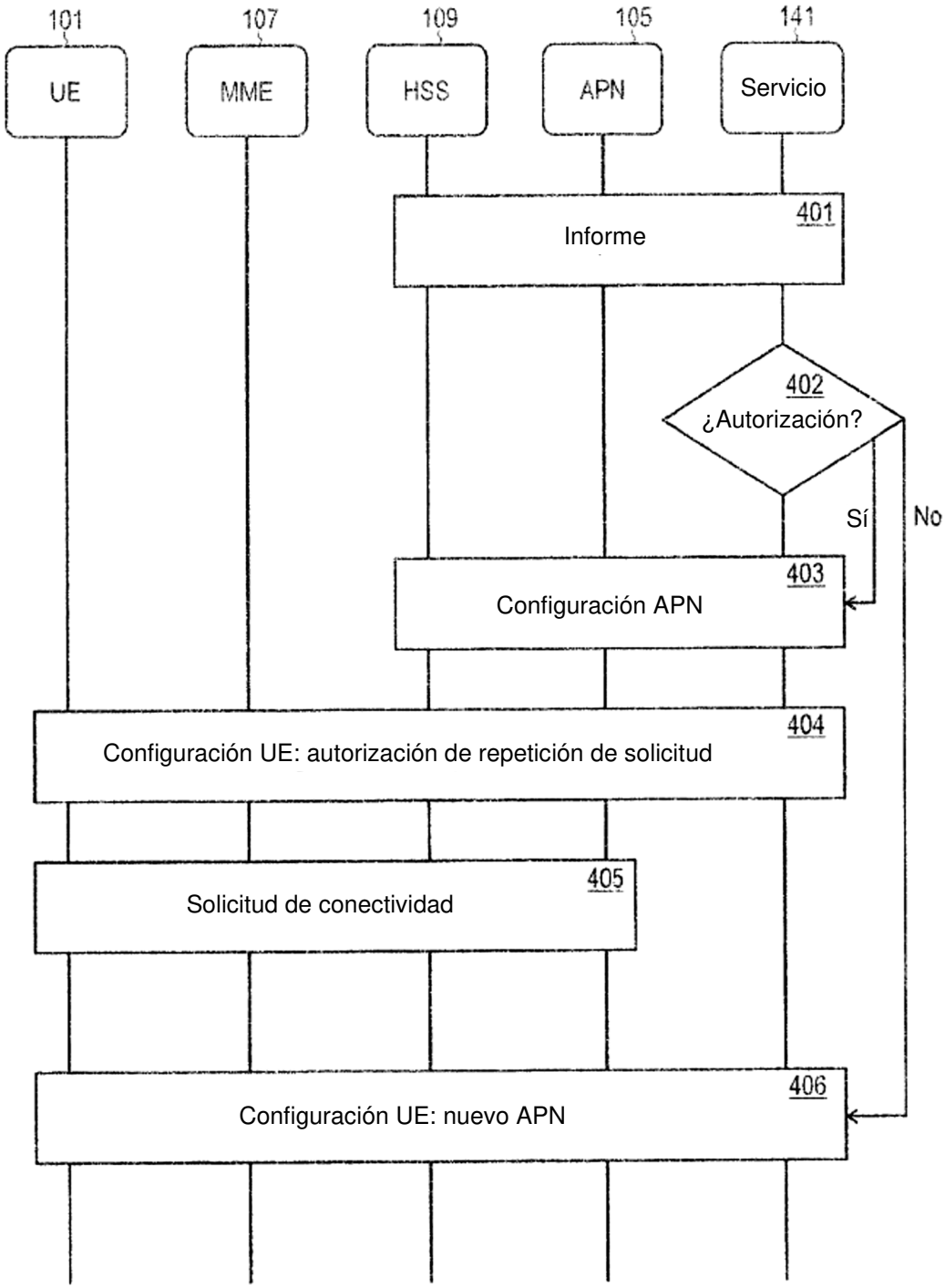
101
107
109
105
141
UE
MME
HSS
APN
Servicio
401
Informe
402
¿Autorización?
Sí
No
403
Configuración APN
404
Configuración UE: autorización de repetición de solicitud
405
Solicitud de conectividad
406
Configuración UE: nuevo APN

Fig. 4

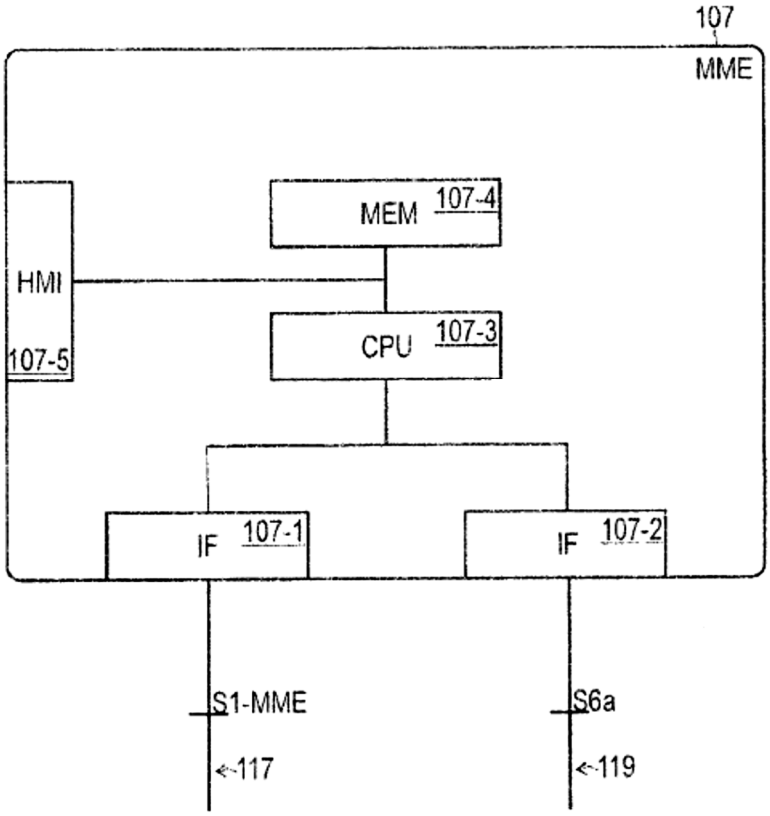
107
MME
MEM 107-4
HMI
107-5
CPU 107-3
IF 107-1
IF 107-2
S1-MME
117
S6a
119

Fig. 5

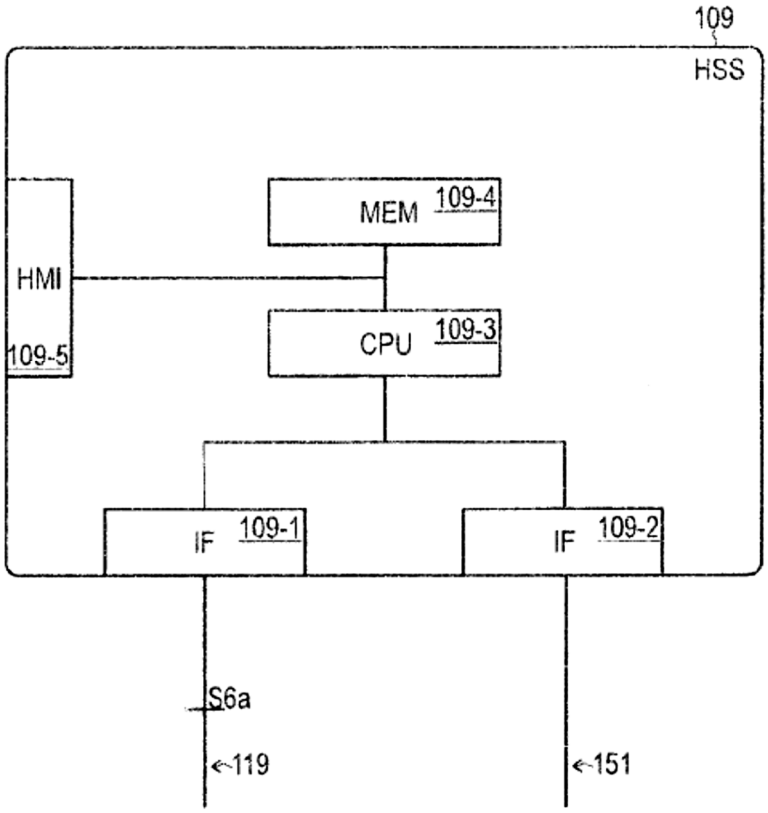


Fig. 6

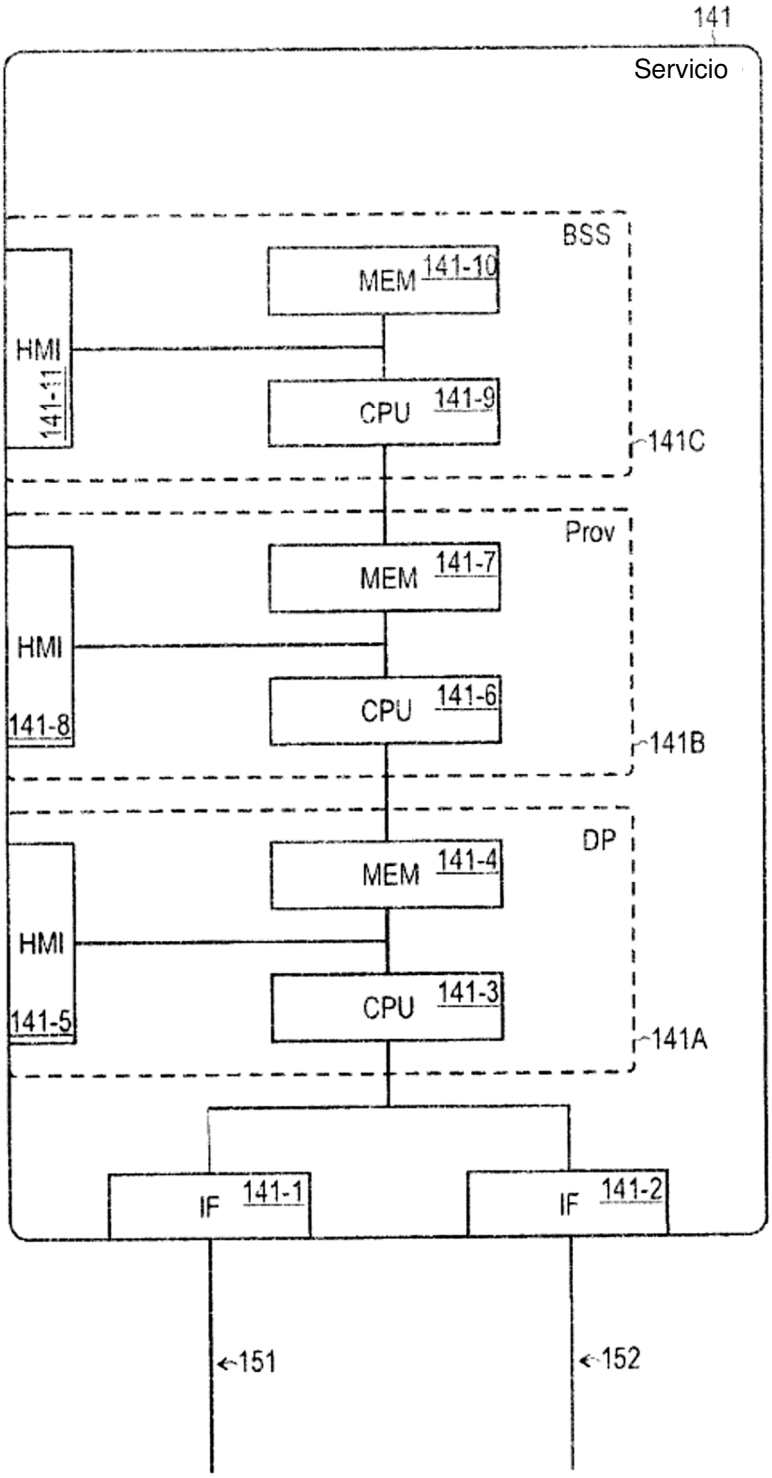
141
Servicio
BSS
MEM 141-10
HMI 141-11
CPU 141-9
141C
Prov
MEM 141-7
HMI 141-8
CPU 141-6
141B
DP
MEM 141-4
HMI 141-5
CPU 141-3
141A
IF 141-1
IF 141-2
151
152

Fig. 7

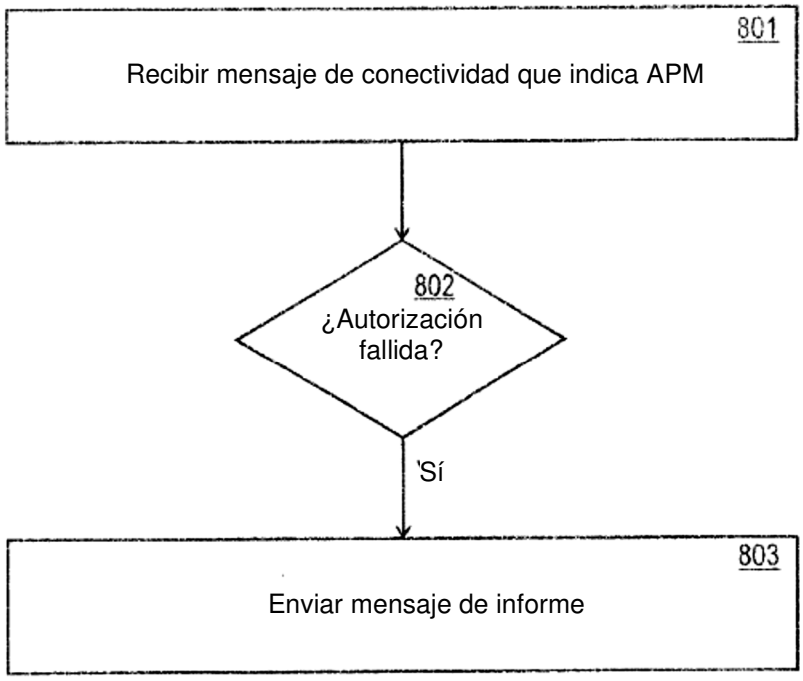
801
Recibir mensaje de conectividad que indica APM
802
¿Autorización fallida?
Sí
803
Enviar mensaje de informe

Fig. 8

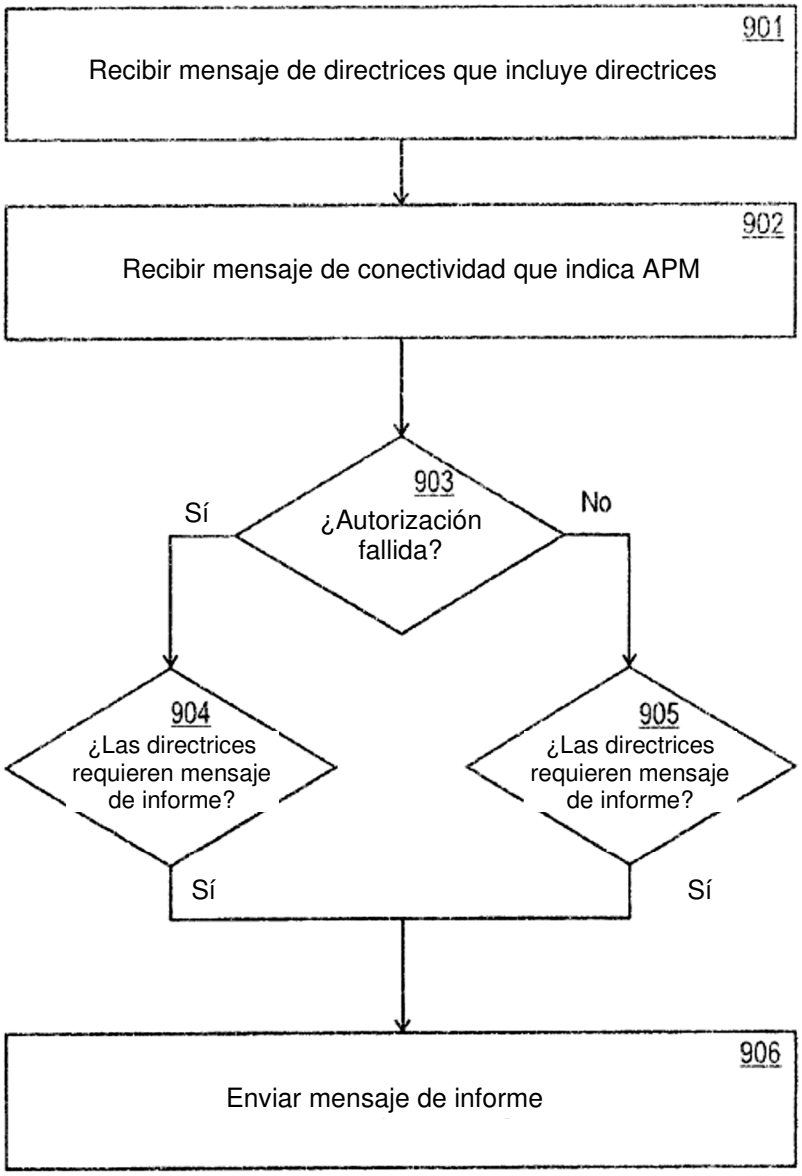
901
Recibir mensaje de directrices que incluye directrices
902
Recibir mensaje de conectividad que indica APM
903
¿Autorización fallida?
Sí
No
904
¿Las directrices requieren mensaje de informe?
905
¿Las directrices requieren mensaje de informe?
Sí
Sí
906
Enviar mensaje de informe

Fig. 9

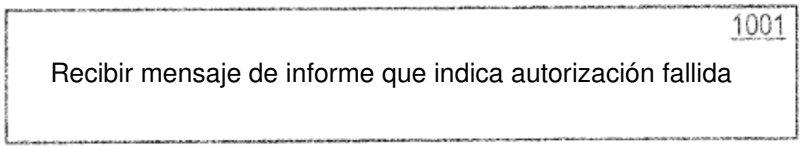
1001
Recibir mensaje de informe que indica autorización fallida

Fig. 10

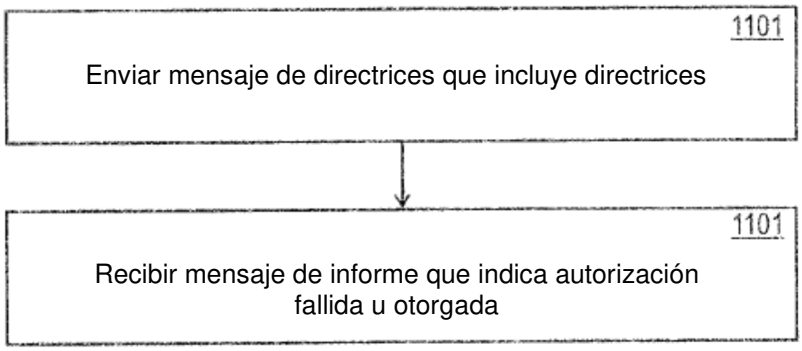
1101
Enviar mensaje de directrices que incluye directrices
1101
Recibir mensaje de informe que indica autorización fallida u otorgada

Fig. 11

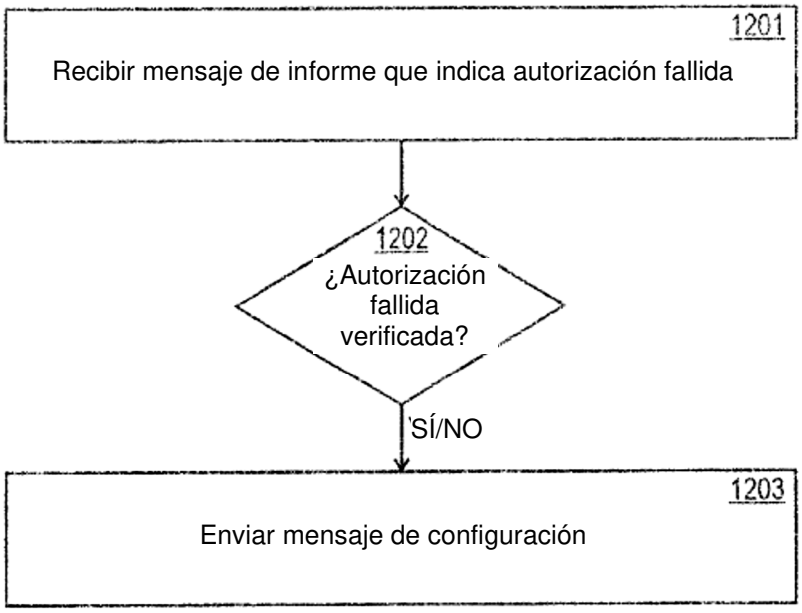
1201
Recibir mensaje de informe que indica autorización fallida
1202
¿Autorización fallida verificada?
SÍ/NO
1203
Enviar mensaje de configuración

Fig. 12