

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 994 210**

51 Int. Cl.:

H04M 15/00 (2014.01)

H04L 12/14 (2014.01)

H04W 4/24 (2014.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **30.09.2021** **E 21200111 (9)**

97 Fecha y número de publicación de la concesión europea: **12.06.2024** **EP 4160992**

54 Título: **Aparatos, métodos y programas informáticos**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
20.01.2025

73 Titular/es:
NOKIA TECHNOLOGIES OY (100.00%)
Karakaari 7
02610 Espoo, FI

72 Inventor/es:
PAPAGEORGIU, APOSTOLOS;
THIEBAUT, LAURENT y
MILINSKI, ALEXANDER

74 Agente/Representante:
DEL VALLE VALIENTE, Sonia

ES 2 994 210 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Aparatos, métodos y programas informáticos

5 **Campo**

La presente descripción se refiere a un aparato, métodos y programas informáticos y, en particular, pero no exclusivamente, a un aparato, métodos y programas informáticos para aparatos de red.

10 **Antecedentes**

Un sistema de comunicación puede verse como una instalación que posibilita sesiones de comunicación entre dos o más entidades, tales como terminales de usuario, nodos de acceso y/u otros nodos, proporcionando recursos para comunicaciones entre las diversas entidades implicadas en la trayectoria de comunicaciones. Un sistema de comunicación se puede proporcionar, por ejemplo, por medio de una red de comunicación y uno o más dispositivos de comunicación compatibles. Las sesiones de comunicación pueden comprender, por ejemplo, comunicación de datos para portar comunicaciones tales como voz, correo electrónico (*e-mail*), mensaje de texto, multimedia y/o datos de contenido, y así sucesivamente. El contenido puede ser multidifusión o unidifusión a dispositivos de comunicación.

Un usuario puede acceder al sistema de comunicación por medio de un dispositivo de comunicación o terminal apropiado. Un dispositivo de comunicación de un usuario se denomina a menudo user equipment (equipo de usuario - UE) o dispositivo de usuario. El dispositivo de comunicación puede acceder a una portadora proporcionada por un nodo de acceso, y transmitir y/o recibir comunicaciones en la portadora.

El sistema de comunicación y dispositivos asociados funcionan típicamente según una norma o especificación requerida que establece lo que se permite que hagan las diversas entidades asociadas con el sistema, y cómo debería conseguirse tal cosa. Los protocolos de comunicación y/o parámetros que se deberán usar para la conexión también se definen de forma típica. Un ejemplo de un sistema de comunicaciones es UTRAN (radio de 3G). Otro ejemplo de una arquitectura conocida es la evolución a largo plazo (LTE) o la tecnología de acceso por radio del Sistema Universal de Telecomunicaciones Móviles (UMTS). Otro sistema de comunicación de ejemplo es el denominado sistema 5G, que permite que un equipo de usuario (UE) o un dispositivo de usuario entren en contacto con un núcleo 5G a través de, p. ej., tecnología de acceso de nueva radio (NR) o mediante otra tecnología de acceso, tal como tecnología de acceso no confiable a 5GC o de acceso por cable. El acceso a un núcleo 5G también se puede proporcionar a través de una red alternativa tal como, por ejemplo, UTRAN o UMTS.

XIAOMI: “eNS_502_KI#5_Update of PDU Session Procedures”, borrador 3GPP, S2-2104319 es una solicitud de cambio relacionada con la actualización de los procedimientos de monitorización y cumplimiento del ancho de banda total por identificador de segmento que se realiza agregando la tasa de bits máxima asignada a cada sesión de unidad de datos de paquetes establecidas en ese segmento identificado.

La publicación de solicitud de patente de los Estados Unidos número US-2021/184875 A1 se refiere a una función de gestión de sesiones que envía, a una función de control de políticas, un mensaje de solicitud de política. El mensaje de solicitud de política comprende un identificador de red no pública de una red no pública a través de la que un dispositivo inalámbrico accede a una red móvil terrestre pública. El mensaje de solicitud de política comprende un identificador de la red móvil terrestre pública. La función de gestión de sesiones recibe, desde la función de control de políticas, un mensaje de respuesta de política que comprende una política de control de cobro.

Resumen

La presente invención se define en las reivindicaciones independientes adjuntas. Ciertos aspectos más específicos se definen por las reivindicaciones dependientes.

Breve descripción de las figuras

Ahora se describirán ejemplos, únicamente a manera de ejemplo, con referencia a las figuras adjuntas, en las que:

las Figuras 1A y 1B muestran una representación esquemática de parte de un sistema 5G de ejemplo;

la Figura 2 muestra una representación esquemática de un aparato de red;

60 la Figura 3 muestra una representación esquemática de un equipo de usuario;

la Figura 4 muestra una representación esquemática de un medio de memoria no volátil que almacena instrucciones que cuando son ejecutadas por un procesador permiten que un procesador realice una o más de las etapas de los métodos de algunos ejemplos;

65

la Figura 5 muestra una representación esquemática de una red;

las Figuras 6 a 11 son diagramas de flujo de señalización que ilustran señalización de ejemplo; y

- 5 las Figuras 12 a 15 son diagramas de flujo que muestran operaciones de ejemplo que pueden realizarse mediante el aparato descrito en la presente memoria.

Descripción detallada

- 10 En lo sucesivo se explican ciertos aspectos con referencia a dispositivos de comunicación móvil capaces de comunicarse a través de un sistema celular inalámbrico y sistemas de comunicación móvil que atienden a tales dispositivos de comunicación móvil. Para mayor brevedad y claridad, a continuación se describen tales aspectos con referencia a un sistema de comunicación inalámbrica 5G. Sin embargo, se entiende que tales aspectos no se limitan a los sistemas de comunicación inalámbrica 5G y pueden, por ejemplo, aplicarse a otros sistemas de comunicación inalámbrica con componentes análogos (por ejemplo, propuestas 6G actuales).

15 3GPP se refiere a un grupo de organizaciones que desarrollan y lanzan diferentes protocolos de comunicación estandarizados. Actualmente, 3GPP está desarrollando y publicando documentos relacionados con la Versión 16, relacionada con la tecnología 5G, y la Versión 17 está actualmente programada para 2022.

20 Antes de explicar en detalle las realizaciones ilustrativas, se explican brevemente ciertos principios generales de un sistema de comunicación inalámbrica 5G con referencia a las Figuras 1A y 1B.

25 La Figura 1A muestra una representación esquemática de al menos parte de un sistema 5G (5GS) 100 de ejemplo. El 5GS puede comprender un equipo 102 de usuario (UE) (que también puede denominarse dispositivo de comunicación o terminal), una red 104 de acceso (AN) 5G (que puede ser una red de acceso por radio (RAN) 5G o cualquier otro tipo de AN 5G, tal como una función de interconexión no 3GPP (N3IWF)/una función de puerta de enlace no 3GPP confiable (TNGF) para acceso no 3GPP no confiable/confiable o una función de puerta de enlace de acceso por cable (W-AGF) para acceso por cable), un núcleo 5G (5GC) 106, una o más funciones 108 de aplicación (AF) y una o más redes 110 de datos (DN).

30 La RAN 5G puede comprender uno o más gNodoB (gNB) o una o más funciones de unidad distribuida gNodoB (gNB) conectadas a una o más funciones de unidad gNodoB (gNB). La RAN puede comprender uno o más nodos de acceso.

35 El 5GC 106 puede comprender una o más funciones 112 de gestión de acceso y movilidad (AMF), una o más funciones 114 de gestión de sesiones (SMF), una o más funciones 116 de servidor de autenticación (AUSF), una o más funciones 118 de gestión de datos unificados (UDM), una o más funciones 120 de plano de usuario (UPF), una o más funciones 122 de repositorio de datos unificados (UDR), una o más funciones 128 de repositorio de red (NRF) y/o una o más funciones 124 de exposición de red (NEF). Si bien la NRF 128 no se representa con sus interfaces, se entiende que esto se debe a motivos de claridad y que la NRF 128 puede tener una pluralidad de interfaces con otras funciones de red.

40 El 5GC 106 también comprende una función 126 de análisis de datos de red (NWDAF). La NWDAF es responsable de proporcionar información de análisis de red previa solicitud procedente de uno o más funciones o aparatos de red dentro de la red. Las funciones de red también pueden suscribirse a la NWDAF 126 para recibir información desde esta. En consecuencia, la NWDAF 126 también está configurada para recibir y almacenar información de red procedente de uno o más funciones o aparatos de red dentro de la red. La recolección de datos mediante la NWDAF 126 se puede realizar basándose en al menos una suscripción a los eventos proporcionados por la al menos una función de red.

45 La red puede comprender, además, un servicio de análisis de datos de gestión (MDAS). El MDAS puede proporcionar análisis de datos de diferentes parámetros relacionados con la red, incluidos, por ejemplo, el nivel de carga y/o la utilización de recursos. Por ejemplo, el MDAS para una función de red (NF) puede recolectar los datos de rendimiento relacionados con la carga de la NF, p. ej., el estado de uso de recursos de la NF. El análisis de los datos recolectados puede proporcionar un pronóstico de información de uso de recursos en un momento futuro predefinido. Este análisis también puede recomendar acciones apropiadas, p. ej., escalado de recursos, control de admisión, equilibrado de carga de tráfico, etc.

50 La Figura 1B muestra una representación esquemática de un 5GC 106' representado en las especificaciones 3GPP actuales.

55 La Figura 1B muestra una UPF 120' conectada a una SMF 114' a través de una interfaz N4. La SMF 114' está conectada a cada una de un UDR 122', una NEF 124', una NWDAF 126', una AF 108', una función 130' de control de políticas (PCF), una AMF 112' y una función de cobro 132' a través de un medio de interconexión que también conecta estas funciones de red entre sí.

60 En el sistema 5G, los datos de política de gestión de sesiones para una sesión de un abonado específico se recupera a partir de los datos de suscripción del abonado específico, almacenándose los datos de suscripción en el repositorio de datos unificados (UDR). Estos datos de política de gestión de sesiones también se denominan "información de

políticas relacionada con la sesión de PDU” en las especificaciones actuales de 3GPP. Los datos de política de gestión de sesiones recuperados son utilizados por la función de política y control (PCF) para determinar diversos detalles de una sesión de PDU del abonado. Esto tiene lugar, principalmente, al establecer la sesión de PDU, pero también puede realizarse durante la vida útil de una sesión de PDU.

Tras recuperar los datos de política de gestión de sesiones para una sesión de un abonado específico, la PCF determina y activa reglas de control de política y cobro (PCC) para una sesión de PDU en la SMF para una pluralidad de finalidades. Por ejemplo, pueden usarse para determinar políticas de calidad de servicio (QoS) y enrutamiento. Como otro ejemplo, las reglas de PCC pueden comprender instrucciones para activar e informar la detección de eventos.

En este segundo ejemplo, la SMF puede ordenar a la UPF que detecte los eventos en cuestión. Esto se puede lograr mediante un procedimiento de suscripción-notificación. Bajo este procedimiento, cuando la UPF detecta un evento al que está suscrito, informa el evento detectado a la SMF. A continuación, la SMF informa la incidencia del evento a la PCF, según la regla de PCC (p. ej., inicio, detención, descripciones de flujo de datos de servicio para el tráfico de aplicación detectado, si es posible, etc.). La PCF puede tomar decisiones de política apropiadas basándose en la información. Estas reglas de PCC (también denominadas políticas en lo sucesivo en la presente memoria) pueden estar relacionadas con una sesión y un abonado específicos.

La recuperación de datos de política de gestión de sesiones mediante la PCF se ilustra con respecto a la Figura 6, que se describe con más detalle a continuación.

La Figura 6 ilustra la señalización que se puede realizar entre una función 601 de gestión de sesiones (SMF), una PCF 602, un UDR 603 y una función 604 de cobro (CHF).

En 6001, la SMF 601 señala la PCF 602. Esta señalización de 6001 es una solicitud para que la PCF cree una política/decisión de política para una sesión particular. Esta política/decisión de política puede ser al menos una regla de PCC. Se entiende que las referencias posteriores a políticas/decisiones de políticas que se determinan también abarcan referencias a las reglas de PCC que se determinan. Usando la terminología de 3GPP actual, esto puede etiquetarse como “Npcf_SMPolicyControl_Create”.

En 6002 y 6003, la PCF 602 y el UDR pueden intercambiar señalización para recuperar información asociada con el abonado que participa en la sesión particular. Estas etapas pueden realizarse cuando la PCF 602 aún no tiene la información relacionada con la suscripción del abonado (p. ej., cuando la solicitud se refiere al establecimiento de una nueva sesión).

Por lo tanto, en 6002, la PCF 602 señala una consulta (por ejemplo, un mensaje Nudr_DM_Query, como se define actualmente en 3GPP) al UDR 603. La PCF 602 recibe una respuesta de suscripción desde el UDR 603 en respuesta a la consulta de 6002 (la respuesta de suscripción puede ser, por ejemplo, un mensaje Nudr_DM_Subscribe, como se define actualmente en 3GPP). El mensaje Nudr_DM_Query enviado al UDR puede comprender un identificador del abonado (p. ej., identificador permanente de suscripción (SUPI), que es un identificador único global de 5G asignado a cada abonado). El mensaje Nudr_DM_Query enviado al UDR puede comprender un nombre de red de datos (DNN) para la sesión. Un DNN es el nombre con el que se conoce a una red externa dentro de una red móvil pública terrestre (PLMN), proporcionando la PLMN acceso al menos a esa red externa. La PLMN puede proporcionar acceso a múltiples redes externas, teniendo cada red externa un DNN asociado. El mensaje Nudr_DM_Query enviado al UDR puede comprender un identificador para el segmento de red utilizado para proporcionar la sesión (p. ej., la información de asistencia para la selección de segmento de red única (S-NSSAI)). El mensaje Nudr_DM_Query enviado al UDR puede comprender, adicionalmente, al menos uno de datos de política para el abonado y/o la sesión, datos de control de política de sesiones de la unidad de datos de protocolo (PDU) y/o datos de uso permitido restante para la sesión y/o el abonado.

En 6004, la PCF 602 recupera información de cobro para el abonado de la sesión a partir de la CHF 604.

En 6005, la PCF 602 toma una decisión de política en dependencia de la información almacenada en la PCF 602 (o en el almacenamiento de memoria accesible de otro modo por la PCF 602) y/o en dependencia de la información recibida a través del intercambio de 6002 a 6003 (cuando se realiza).

En 6006, la PCF 602 responde a la señalización de 6001 devolviendo la decisión de política determinada en 6005.

Los datos de política de gestión de sesiones pueden comprender diversas políticas estáticas fijadas en la suscripción del abonado. Estas políticas estáticas pueden comprender, por ejemplo, una lista de servicios a los que el abonado puede acceder, la GBR (tasa de bits garantizada) suscrita, los límites de uso, etc. Sin embargo, los datos de política de gestión de sesiones también pueden comprender una parte dinámica que está relacionada con la monitorización de uso, tal como el “uso permitido restante”. El “uso permitido restante” se actualiza durante la vida útil de una sesión de PDU basándose en los informes de uso que la PCF recibe desde la función de plano de usuario (UPF) a través de la función de gestión de sesiones (SMF). Esto se ilustra en la Figura 7.

ES 2 994 210 T3

La Figura 7 ilustra la señalización que se puede realizar entre una SMF 701, una PCF 702, un UDR 703, una función de aplicación (AF) 704 y una CHF 705.

5 En 7001, la SMF 701 señala una solicitud de actualización de política a la PCF 702. Usando la terminología actual, este mensaje puede ser una solicitud Npcf_SMPolicyControl_Update.

10 En 7002, la PCF 702 intercambia señalización con la función de aplicación 704 para informar que se ha producido un evento identificado por las reglas de PCC y/o para informar información identificada en las reglas de PCC como de interés para la función de aplicación 704. Como se mencionó brevemente antes, además del enrutamiento y/o la información relacionada con OoS, las reglas de PCC pueden comprender indicaciones de eventos sobre los que se debe realizar el informe. Los informes de eventos se realizan cuando se cumplen los criterios de umbral comprendidos en las reglas de PCC para la sesión de un abonado. Por lo tanto, se puede decir que los criterios de umbral definen criterios que, cuando se cumplen, desencadenan el envío de un mensaje de informe a la PCF que informa a la PCF que se han cumplido los criterios de umbral. Este criterio de umbral puede ser simplemente una determinación de que se ha producido un evento particular. Este criterio de umbral puede ser una determinación de que se ha producido una combinación particular de eventos. Por lo tanto, se puede decir que este criterio de umbral es una indicación de un evento y/o información sobre la que la función de aplicación desearía recibir información. En 7003, la PCF 703 intercambia señales con la CHF 705 para recuperar un informe de límite de gasto que indica cuánto cobro se ha realizado en la sesión hasta el momento, basándose en la información recibida en 7001.

20 En 7004, la PCF 702 toma una decisión de política basándose en la información determinada en 7001 y 7003. Por ejemplo, usando la terminología de 3GPP actual, cuando la SMF 701 informó un uso acumulado para la sesión de PDU en 7001, la PCF 702 deduce el valor a partir del uso permitido restante para el abonado, el DNN y la S-NSSAI en el UDR invocando la operación de servicio Nudr_DM_Update. En esencia, esta decisión de política solicita que el UDR utilice algunos “datos actualizados” comprendidos en la decisión de política para actualizar un valor/atributo de uso permitido restante dentro de los datos de política que están asociados con ciertos parámetros. Los parámetros pueden ser, por ejemplo: SUPI, DNN y S-NSSAI.

25 En 7005, la PCF 702 señala la decisión de política determinada en 7004 a la SMF 702. Usando la terminología de 3GPP actual. Esto puede ser una respuesta a la solicitud de actualización de 7001. Esto se puede realizar usando una respuesta Npcf_SMPolicyControl_Update.

30 Actualmente, debido a que los datos de la política de gestión de sesiones son propiedad y se manejan únicamente mediante la red móvil pública terrestre doméstica (HPLMN), la monitorización de uso no es aplicable en ciertos casos de itinerancia, tal como, por ejemplo, el caso de itinerancia de ruptura local (LBO) en 5G. Por brevedad, a continuación se considera la itinerancia desde un caso de LBO. Sin embargo, se entiende que esto se utiliza como ejemplo y que la presente discusión también se aplica a otros casos de itinerancia. Por ejemplo, en los casos de 4G, la parte dinámica de la política no puede realizarse únicamente mediante entidades ubicadas dentro de una red móvil pública terrestre visitada (VPLMN); en estos casos, se realiza una interacción con la HPLMN. Además, por simplicidad, lo siguiente se refiere a las PLMN visitadas y domésticas. Sin embargo, se entiende que las técnicas descritas en la presente memoria pueden aplicarse a diferentes dominios.

35 El 4G planteó la posibilidad de contar con una monitorización de uso en los casos de LBO que realiza la HPLMN. Esto utilizaría la denominada interfaz S9 entre una función de política y reglas de cobro (PCRF) doméstica (es decir, la PCRF en HPLMN) y una PCRF visitada (es decir, la PCRF en VPLMN), que se discute más adelante.

40 . En la ruptura local, un usuario que realiza movilidad dentro y a través de una región de red definida por el operador tiene su enrutamiento optimizado de modo que el tráfico de plano de usuario no tiene que abandonar la región actual. La ruptura local también es una característica de las redes 5G y puede utilizarse en estándares de comunicaciones 3GPP posteriores (p. ej., 6G, etc.). La ruptura local se admite en algunas redes 3GPP mediante el uso de una interfaz S9 entre una función de política y reglas de cobro doméstica y una función de política y reglas de cobro visitada. Esta interfaz se utiliza para transferir decisiones de políticas (p. ej., reglas de control de cobro de política (PCC) y/o reglas de calidad de servicio) que se generaron en la red doméstica para su aplicación en la red visitada y para transportar eventos que pueden producirse en la red visitada a la red doméstica. En general, una función de política y reglas de cobro (PCRF) soporta la detección de flujo de datos de servicio, el cumplimiento de políticas y el cobro basado en flujo.

45 En mayor detalle, en las especificaciones 3GPP de 4G/núcleo de paquetes evolucionado (EPC), existe una interfaz S9 entre la PCRF de la HPLMN y la PCRF de la VPLMN. Esto puede utilizarlo la VPLMN para recuperar políticas a partir de la HPLMN, incluidas políticas relacionadas con la información de monitorización de uso en la situación de itinerancia con ruptura local.

50 Por lo tanto, la monitorización de uso y las reacciones apropiadas (relacionadas con las políticas) son posibles en las sesiones de PDU de LBO en 4G/EPC, y se podría aplicar una solución equivalente en redes de comunicación 5G, desempeñando la PCF el papel de PCRF y desempeñando el UDR el papel de SPR (repositorio de perfiles de abonados), e introduciéndose la funcionalidad relacionada de la interfaz S9 en la interfaz N24, que es la interfaz 5G entre la PCF de la HPLMN y la PCF de la VPLMN.

Sin embargo, basándose en este procedimiento, la monitorización de uso se realizaría en la HPLMN de todos modos. Esto daría lugar a una gran cantidad de señalización entre PLMN, un uso excesivo de recursos de red, falta de políticas determinadas por VPLMN y reacciones de PCF lentas a eventos de SMF.

Además, el uso de la interfaz S9 en redes LTE no se implementó finalmente en el EPC debido a que los operadores querían limitar la señalización a través de las interfaces entre operadores al mínimo indispensable para minimizar la congestión de la red.

Como observación, cabe señalar que, si bien el 5GC utiliza una interfaz PCF-PCF entre PLMN, que está etiquetada como N24 en las especificaciones 3GPP, esta interfaz se refiere a las PCF que sirven a la AMF (es decir, a la gestión de políticas a nivel de UE), mientras que la monitorización de uso implicaría que las PCF sirvan a la SMF (gestionando políticas a nivel de sesión de PDU) y, a menudo, se implementan diferentes PCF para servir a la AMF en comparación con las PCF implementadas para servir a la SMF.

Además, en todos los casos de 5G y 4G, no existe ningún mecanismo para realizar la monitorización de uso en la VPLMN, lo que significa que la VPLMN no maneja ni monitoriza ningún límite de uso y no tiene impacto en las acciones que se pueden realizar basándose en tales límites.

Dado que la VPLMN actualmente no tiene ningún mecanismo técnico para aplicar políticas basadas en el uso, esto impide que las entidades de la VPLMN puedan ayudar a impedir casos de uso de datos excesivo por parte de los itinerantes al reaccionar ante la superación de un límite de uso determinado por HPLMN. La VPLMN actual tampoco tiene actualmente ningún mecanismo técnico para proteger la red VPLMN de la sobrecarga provocada por itinerantes entrantes al reaccionar ante la superación de los límites de uso determinados por VPLMN.

Para abordar al menos uno de los problemas mencionados anteriormente, a continuación se describe un mecanismo para realizar la monitorización de uso en la VPLMN y hacer cumplir las políticas determinadas por VPLMN. Estas políticas pueden aplicarse cuando la sesión alcanza ciertos límites de uso en las sesiones de PDU de usuarios que están en itinerancia en modo de ruptura local.

En particular, la VPLMN descrita a continuación puede determinar límites de uso para un itinerante ante el establecimiento de la sesión de PDU. Estos límites de uso pueden determinarse de varias maneras diferentes. Por ejemplo, los límites de uso pueden recuperarse con una única interacción a partir de la HPLMN y pueden ser específicos de la combinación abonado-VPLMN. Como otro ejemplo, los límites pueden almacenarse localmente en la VPLMN y ser comunes para todos los abonados de la HPLMN.

La VPLMN puede configurarse para utilizar entradas de base de datos dinámicas/temporales de datos de política de gestión de sesiones con el fin de monitorizar el uso restante permitido de la sesión de PDU. Esta información puede proporcionarse a través de, por ejemplo, un UDR.

Como ejemplo del uso de entradas de base de datos dinámicas, la VPLMN puede configurarse para realizar un seguimiento del uso permitido restante usando informes de uso enviados desde la UPF hasta la SMF hasta la V-PCF hasta el UDR en la VPLMN. Este proceso puede complementarse con un mecanismo para restablecer y/o eliminar entradas basándose en el período de tiempo durante el que se aplican los límites de uso. Este mecanismo complementario puede usarse para permitir que las entradas de datos de política de gestión de sesiones de los itinerantes sean temporales en la VPLMN.

Estos conceptos se ilustran con más detalle en los ejemplos que se discuten a continuación.

A continuación, se describen ejemplos en los que los procedimientos de establecimiento de asociación de política de gestión de sesiones y modificación de asociación de política de gestión de sesiones iniciados por SMF descritos anteriormente se modifican para comprender una secuencia de interacciones y algunos elementos que pueden usarse en el caso de itinerancia y permitir la monitorización de uso realizada por VPLMN (y el cumplimiento de políticas basado en monitorización).

A continuación, las Figuras 8 y 9 muestran ejemplos de cómo se pueden obtener los límites de uso en un caso inicial. Por ejemplo, la Figura 8 muestra un ejemplo en el que una PCF en la VPLMN recupera un valor para el límite de uso basándose en una combinación de un identificador para el abonado y un identificador para la VPLMN. La Figura 9, por el contrario, ilustra un ejemplo en el que una V-SMF recupera información de límite de uso a partir de una H-UDM.

Además, la Figura 10 ilustra un ejemplo de cómo se puede crear una política cuando se recupera información de uso a partir de la información de suscripción de un abonado que se almacena en un V-UDR, mientras que la Figura 11 ilustra un ejemplo de cómo se puede realizar una solicitud de actualización para actualizar la información de suscripción que se almacena en el V-UDR para el abonado. La información de suscripción puede ser, por ejemplo, un "uso permitido restante". La Figura 11 ilustra, además, las etapas que se pueden realizar cuando se elimina al menos

parte de la información de suscripción. La información de suscripción puede eliminarse una vez transcurrido un “tiempo de restablecimiento” en la PLMN visitada. Esto se discute más adelante.

5 La Figura 8 ilustra una señalización potencial entre una SMF visitada (V-SMF) 801, una PCF visitada (V-PCF) 802, un UDR visitado (V-UDR) 803, una PCF doméstica (H-PCF) 804 y un UDR doméstico (H-UDR) 805. La V-SMF 801, la V-PCF 802 y el V-UDR 803 están ubicados en una misma VPLMN. La H-PCF 804 y el H-UDR están ubicados en el mismo H-PLMN con el que está asociado el abonado asociado con la sesión. Este ejemplo de la Figura 8 se refiere a la señalización entre PCF.

10 En 8001, la V-SMF 801 señala una solicitud a la V-PCF 802 para crear una decisión de política para una sesión particular. Usando la terminología de 3GPP actual, esto se puede realizar usando un mensaje de solicitud Npcf_SMPolicyControl_Create.

15 Cuando la V-PCF 802 determina que esta solicitud se refiere a un caso de LBO y que es probable que el V-UDR 803 comprenda una entrada de datos de política de gestión de sesiones dinámica aplicable para la sesión de PDU que este itinerante con LBO ha establecido, se realizan 8002 y 8003.

20 En 8002, la V-PCF 802 señala una consulta al V-UDR 803. La consulta puede señalizarse invocando Nudr_DM_Query. Esta consulta puede comprender al menos uno de: un identificador para el abonado (p. ej., SUPI), un identificador del DNN, un identificador del segmento relevante para esta sesión (p. ej., S-NSSAI), datos de política relacionados con la sesión, datos de control de política de sesiones de PDU relacionados con la sesión y cualquier dato de uso permitido restante.

25 En 8003, el V-UDR 803 puede responder a la consulta recibida en 8002 con datos actuales sobre este itinerante. Esta información puede incluir información relacionada con los datos de uso permitido restante actuales.

30 Cuando la V-PCF 802 determina que es poco probable que el V-UDR 803 comprenda una entrada de datos de política de gestión de sesiones dinámica aplicable para la sesión de PDU que este itinerante con LBO ha establecido, o cuando 8003 no comprende ninguna información relacionada con los datos de uso permitido restante actuales, se realizan 8004 a 8006.

35 En 8004, la V-PCF 802 señala una solicitud de decisión de política a la H-PCF 804. Esta solicitud de decisión de política puede solicitar datos de política de gestión de sesiones que se aplican cuando el abonado indicado (indicado, por ejemplo, por un SUPI) desea acceder a la combinación de una red de datos indicada (indicada, por ejemplo, por un DNN) e información de segmento (indicada, por ejemplo, por un S-NSSAI proporcionado) de la red del dominio indicado (p. ej., la VPLMN indicada). Esta señal puede ser, por ejemplo, una solicitud Npcf_SMPolicyControl_Create. En cambio, esta señal puede señalizarse usando una nueva operación, etiquetada, en la presente memoria, como Npcf_SMPolicyControl_Get. Esta solicitud de decisión de política puede señalizarse en la interfaz N24 entre V-PCF y H-PCF.

40 En 8005, la H-PCF 804 envía una consulta al H-UDR 805. La consulta puede señalizarse invocando Nudr_DM_Query. Esta consulta puede comprender al menos uno de: un identificador para el abonado (p. ej., SUPI), un identificador del DNN, un identificador del segmento relevante para esta sesión (p. ej., S-NSSAI), datos de política relacionados con la sesión, datos de control de política de sesiones de PDU relacionados con la sesión y cualquier dato de uso permitido restante. Además, la consulta puede comprender una indicación de la identidad de la VPLMN (es decir, la PLMN dentro de la que se encuentran la V-PCF, el V-UDR y la V-SMF). En otras palabras, la H-PCF 804 intenta recuperar los datos de política de gestión de sesiones (incluidos los límites de uso) que se aplicarán a la combinación SUPI y VPLMN-ID en cuestión a partir del H-UDR 805. Esta información de límite de uso es por UE y PLMN y, por lo tanto, es un nuevo dato de política que se definirá en los conjuntos de datos expuestos por el UDR.

50 Si bien no se muestra, el H-UDR 805 puede responder a la consulta de 8005 con datos de uso actuales relacionados con la sesión.

55 En 8006, la H-PCF 804 responde a la señalización de 8004 con datos de política de gestión de sesiones. Por lo tanto, esta señalización se puede realizar usando una respuesta Npcf_SMPolicyControl_Create (o a través de la nueva respuesta de mensaje, tal como la respuesta Npcf_SMPolicyControl_Get). Esta señalización puede comprender límites de uso. Por ejemplo, esta respuesta puede comprender límites de uso para el abonado. Alternativamente o además, esta respuesta puede comprender un tiempo de restablecimiento, que se define en la presente memoria. Se considera que el tiempo de restablecimiento es un tiempo después del que la PLMN que realiza la monitorización restablece el valor del “uso permitido restante” de regreso al valor del límite inicial. En otras palabras, el tiempo de restablecimiento indica un tiempo después del que el uso permitido restante para la sesión de PDU se restablecerá a los límites proporcionados. En particular, cuando se alcanza el “tiempo de restablecimiento” de una suscripción, la V-PCF puede solicitar que el V-UDR elimine los datos de política relacionados con la suscripción. Esto se discute más adelante en relación con la Figura 11.

65 Si bien no se muestra en la Figura 8, la V-PCF 802 puede realizar una decisión de política como se ha descrito anteriormente en relación con las acciones de la PCF descritas en la Figura 6 y/o la Figura 7. Además, la V-PCF 802 puede responder a

la solicitud recibida en 8001 respondiendo a la V-SMF con una respuesta Npcf_SMPolicyControl_Create como se ha descrito anteriormente en relación con la Figura 6 y/o la Figura 7.

5 La Figura 9 ilustra una señalización de ejemplo que se puede realizar cuando la VPLMN maneja el control de límite de uso sin involucrar a la HPLMN.

10 La Figura 9 ilustra una señalización potencial entre un UE 901, una red 902 de acceso por radio (RAN), una función 903 de acceso y movilidad (AMF), una función 904 de plano de usuario, una SMF 905, una PCF 906, un UDM 907 y una red 908 de datos (DN). Todas las entidades de red de núcleo representadas en la Figura 9 forman parte de la VPLMN, salvo el UDM 907, que forma parte de la PLMN doméstica. En otras palabras, al menos AMF 903, UPF 904, SMF 905, PCF 906 y UDM 907 son entidades de la VPLMN.

15 En 9001, el UE señala una solicitud de establecimiento de sesión a la AMF 903. Esto se puede realizar, por ejemplo, usando señalización de estrato de no acceso (NAS). La solicitud de establecimiento de sesión puede ser una solicitud de establecimiento de sesión de PDU.

En 9002, la AMF 903 señala la SMF 905 para crear una sesión para el abonado del UE 901. Usando la terminología de 3GPP actual, esta solicitud puede ser una solicitud Nsmf_PDU Session CreateSMContext.

20 En 9003, la SMF 905 señala el UDM 907 para recuperar información de suscripción para el abonado del UE 901. Usando la terminología de 3GPP actual, la solicitud de información de suscripción puede ser, por ejemplo, una solicitud Nudm_SDM_Get. Esta solicitud puede comprender: un identificador para el abonado (p. ej., SUPI), datos de suscripción de gestión de sesiones para la sesión, un identificador de un nombre de red de datos seleccionado e información de segmento para la sesión (p. ej., S-NSSAI), un identificador de la VPLMN y el identificador de red (p. ej., un DNN). La SMF 905 puede suscribirse, además, a cambios en esta información. Esto se puede realizar utilizando la señalización Nudm_SDM_Subscribe.

30 En 9004, el UDM 907 determina la información de límite de uso para la sesión solicitada después de determinar que se aplica una situación de LBO. El límite de uso puede indicar una asignación de tamaño para los datos usados por un abonado. Por ejemplo, en un ejemplo de 500 megabytes, cuando un abonado ha utilizado 500 MB de datos durante una sesión, entonces se puede informar a la PCF sobre un evento. Se entiende que el límite de uso puede expresarse en términos de otros valores, tal como una cantidad de datos usados dentro de un período de tiempo predeterminado.

35 En 9005, la UDM 907 responde a la señalización de 9003. Usando la terminología de 3GPP actual, esta respuesta puede ser una respuesta Nudm_SDM_Get. En comparación con instancias anteriores de este mensaje, este mensaje puede configurarse para comprender la información de límite de uso determinada en 9004.

40 En 9006, la SMF 905 señala una solicitud a la PCF 902 para crear una decisión de política para una sesión particular. Usando la terminología de 3GPP actual, esto se puede realizar usando un mensaje de solicitud Npcf_SMPolicyControl_Create. Sin embargo, en comparación con instancias anteriores de este mensaje, este mensaje puede configurarse para incluir el límite de uso recibido en 9005.

45 **En** 9007, la PCF 906 determina una decisión de política en respuesta a la señalización de 9006. Esta determinación puede realizarse dependiendo del límite de uso recibido de 9006. El resto de esta determinación se puede realizar como una decisión de política como se ha descrito anteriormente en relación con las acciones de la PCF descritas en la Figura 6 y/o la Figura 7. La PCF 906 puede realizar, además, las acciones que se describen a continuación en relación con las etapas de la Figura 11. Como alternativa a la realización de estas etapas de la Figura 11, la PCF 906 puede esperar un primer informe de uso procedente de la SMF 905.

50 **En** 9008, la PCF 906 puede responder a la solicitud recibida en 9006 respondiendo a la V-SMF con una respuesta Npcf_SMPolicyControl_Create como se ha descrito anteriormente en relación con la Figura 6 y/o la Figura 7.

La Figura 10 ilustra una señalización potencial entre una V-SMF 1001, una V-PCF 1002 y un V-UDR 1003.

55 En 10001, la V-SMF 1001 señala una solicitud de una política para una sesión a la V-PVF 1002. Usando la terminología de 3GPP actual, esto se puede realizar usando un mensaje de solicitud Npcf_SMPolicyControl_Create.

60 Cuando la V-PCF 802 determina que esta solicitud se refiere a un caso de LBO y que es probable que el V-UDR 803 comprenda una entrada de datos de política de gestión de sesiones dinámica aplicable para la sesión de PDU que este itinerante con LBO ha establecido, se realizan 8002 y 8003.

65 En 10002, la V-PCF 1002 envía una consulta al V-UDR 803. La consulta puede señalizarse invocando Nudr_DM_Query. Esta consulta puede comprender al menos uno de: un identificador para el abonado (p. ej., SUPI), un identificador del DNN, un identificador del segmento relevante para esta sesión (p. ej., S-NSSAI), datos de política relacionados con la sesión, datos de control de política de sesiones de PDU relacionados con la sesión y cualquier dato de uso permitido restante.

ES 2 994 210 T3

En 10003, el V-UDR 1003 puede responder a la consulta recibida en 10002 con datos actuales sobre este itinerante. Esta información puede incluir información relacionada con los datos de uso permitido restante actuales.

5 **Cuando** la V-PCF 1002 determina que la señalización de 10003 no comprende ninguna información relacionada con los datos de uso permitido restante actuales y la V-PCF 1002 determina que no existe ningún acuerdo para que la V-PCF recupere los límites de uso de usuario a partir de la HPLMN del abonado, se realizan 10004 a 10005.

10 En 10004, la V-PCF 1003 señala una consulta al V-UDR 1004. Esta consulta señalizada se puede realizar invocando una solicitud Nudr_DM_Query que comprende un identificador de la HPLMN e información relacionada con la sesión de PDU a la que se refiere la política solicitada (p. ej., el nombre de red de datos y/o la información de segmento (p. ej., la S-NSSAI) de la sesión de PDU).

15 **En** 10005, el V-UDR 1004 responde a la consulta de 10004. Esta respuesta puede comprender límites de uso que se aplicarán a la sesión de PDU establecida. Esta respuesta puede comprender una identificación del tiempo de restablecimiento. Como se ha mencionado anteriormente, el tiempo de restablecimiento se considera un tiempo respectivo después del que el uso permitido restante para la sesión de PDU se restablecerá a los límites proporcionados.

20 En 10006, la V-PCF 1002 realiza una decisión de política como se ha descrito anteriormente en relación con las acciones de la PCF descritas en la Figura 6 y/o la Figura 7.

En 10007, la V-PCF 1002 puede responder a la solicitud recibida en 10001 respondiendo a la V-SMF con una respuesta Npcf_SMPolicyControl_Update como se ha descrito anteriormente en relación con la Figura 6 y/o la Figura 7.

25 La Figura 11 ilustra una señalización potencial entre una V-SMF 1101, una V-PCF 112 y un V-UDR 1103 después de que se hayan realizado las operaciones de al menos una de las Figuras 8 a 10 (es decir, después de que la V-PCF haya determinado con éxito un tiempo de restablecimiento y/o un uso restante).

30 En 11001, la V-PCF 1102 determina que ha expirado un tiempo de restablecimiento y señala el V-UDR 1103 en respuesta a esta determinación. Esta señalización está configurada de modo que el V-UDR elimine la entrada dinámica para una combinación de dominio abonado-PLMN del V-UDR 1103 (proporcionada a la V-PCF 1102 como se discute en los ejemplos anteriores de las Figuras 8 a 10). Por lo tanto, esta señalización puede comprender una indicación del abonado (p. ej., el SUPI para el abonado) y al menos uno del nombre de red de datos y/o el identificador de segmento para la sesión. La señalización puede comprender una indicación de que el UDR debe eliminar datos de política almacenados para una combinación indicada de un abonado (p. ej., indicada a través de un SUPI proporcionado en la solicitud), una red de datos (p. ej., indicada a través de un DNN proporcionado) e información de segmento para la sesión (p. ej., indicada a través de una S-NSSAI proporcionado en la solicitud). La señalización puede etiquetarse como Nudr_DM_Delete.

40 En 11002, la V-SMF 1101 señala una solicitud de actualización de control de política a la V-PCF 1102. Esta solicitud de actualización puede etiquetarse como Npcf_SMPolicyControl_Update. La señalización de 11002 se puede realizar cuando se ha cumplido una condición de activación de solicitud de control de política. Esta señalización puede comprender información sobre el uso de datos (p. ej., que hasta el momento se ha utilizado X cantidad de datos durante esta sesión) y una indicación de una sesión en la que resulta el uso de datos.

45 Cuando la señalización de 11002 comprende un informe de uso, la V-PCF realiza 11003.

50 En 11003, la V-PCF 1102 determina si la combinación de dominio abonado-PLMN proporcionada en 11002 está actualmente almacenada en el V-UDR 1103. Cuando la combinación de dominio abonado-PLMN no está almacenada en el V-UDR, la solicitud de 11002 se refiere a un nuevo itinerante o para itinerantes cuyas entradas anteriores han expirado y, por lo tanto, se han eliminado (tal como sucedió en 11001). Cuando la combinación de dominio abonado-PLMN se almacena en el V-UDR, la solicitud de 11002 se refiere a un itinerante existente. Esto puede determinarse mediante la V-PCF 1102 al señalar una consulta (p. ej., Nudr_DM_Query) al V-UDR 1103 a este efecto y al recibir una respuesta.

55 Cuando la solicitud de 11002 se refiere a un caso en el que no hay ninguna combinación de abonado-PLMN almacenada en el V-UDR 1103, se envía una solicitud de “creación” al V-UDR para hacer que el V-UDR almacene la combinación abonado-PLMN de 11002 en el V-UDR 1103. La solicitud de creación puede comprender un identificador del abonado (p. ej., un SUPO), una indicación de un DNN, una indicación de una identificación de segmento (p. ej., una S-NSSAI), datos de política, una indicación de datos de uso permitido restante y/o cualquier dato recibido al establecer la sesión. Los límites de uso recibidos al establecer la asociación de políticas de SM se pueden usar como valores iniciales del “uso permitido restante” (para todas las métricas de límite de uso posibles, p. ej., basadas en tiempo o basadas en datos).

65 En 11004, la V-PCF 1102 realiza un procedimiento de actualización para actualizar información actualmente en el V-UDR 1103 sobre esta combinación abonado-PLMN. Este procedimiento de actualización se realiza para sustraer el uso recibido en el informe de uso de 11002 del “uso permitido restante”.

En 11005, la V-PCF 1102 toma una decisión de política.

En 11006, la V-PCF 1102 señala la decisión de política determinada en 11005 a la V-SMF 1101.

5 Las Figuras 12 a 15 son diagramas de flujo que ilustran ciertas características de los ejemplos descritos anteriormente. Por lo tanto, se entiende que las características descritas a continuación se pueden combinar con características más específicas descritas en los ejemplos discutidos anteriormente.

10 La Figura 12 ilustra operaciones que pueden realizarse mediante un aparato para una primera función de control de políticas. La primera función de control de políticas puede configurarse para operar en un primer dominio. El primer dominio puede ser un dominio visitado por un abonado en itinerancia. En un caso de este tipo, la primera función de control de políticas puede ser una VPCF.

15 En 1201, el aparato recibe, desde una función de gestión de sesiones, una solicitud para que se establezca una política para una sesión para un abonado (p. ej., el abonado en itinerancia), en donde el abonado está suscrito en un segundo dominio (p. ej., el dominio doméstico del abonado) y la primera función de control de políticas está configurada para operar en un primer dominio (p. ej., el dominio visitado).

20 En 1202, el aparato determina una política para la sesión solicitada, comprendiendo la política determinada una indicación de un uso permitido para el abonado y al menos una condición de activación para que la política se actualice. Como ejemplo, el usuario puede tener un uso permitido de X MB por día mientras está conectado al segundo dominio. En este ejemplo, hay un uso permitido de X MB y un tiempo de restablecimiento de un día (p. ej., todos los días, el “uso permitido restante” se restablecerá a X MB, aunque puede disminuir durante su uso durante el día).

25 En 1203, el aparato señala al menos una condición de activación a la función de gestión de sesiones.

En 1204, el aparato monitoriza el uso permitido para el abonado actualizando la política en respuesta a la recepción de una indicación de que se ha cumplido al menos una condición de activación. Esto puede comprender la actualización del “uso permitido restante”, según el ejemplo anterior.

30 La determinación de una política puede comprender señalar, a una segunda función de control de políticas que opera en el segundo dominio, una solicitud para el uso permitido, comprendiendo la solicitud una identificación del abonado y una identificación de la conectividad de datos que se solicita. La identificación de la conectividad de datos que se solicita puede comprender un DNN e información de identificación de segmento para la sesión (p. ej., S-NSSAI). El aparato puede recibir el uso permitido desde la segunda función de control de políticas.

35 El aparato puede señalar, a una función de repositorio de datos configurada para operar en el primer dominio, una solicitud para el uso permitido. El aparato puede recibir una indicación desde la función de repositorio de datos de que el uso permitido no está disponible en el repositorio de datos. En un caso de este tipo, la señalización a la segunda función de control de políticas, se puede realizar una solicitud para el uso permitido en respuesta a la indicación recibida desde la función de repositorio de datos.

40 La determinación de una política puede comprender señalar, a una función de repositorio de datos que opera en el primer dominio, una solicitud de una cantidad restante del uso permitido, comprendiendo la solicitud una identificación del abonado. El aparato puede recibir una indicación del uso permitido desde la función de repositorio de datos.

45 La solicitud de una política para que se establezca una sesión para un abonado puede comprender la indicación del uso permitido.

50 La monitorización puede comprender recibir, desde la función de gestión de sesiones, una indicación de que se ha cumplido al menos una condición de activación; y señalar, a una función de repositorio de datos configurada para operar en el mismo dominio que la primera función de control de políticas, una solicitud para actualizar una información de uso para el abonado que se almacena mediante la función de repositorio de datos.

55 La monitorización puede comprender, en respuesta a recibir dicha indicación de que se ha cumplido al menos una condición de activación, recuperar información que identifica una cantidad del uso permitido que resta después de que se cumpla la condición de activación, en donde dicha señalización de la solicitud para actualizar la política comprende una solicitud para actualizar el uso permitido. Como ejemplo, la solicitud puede ser una solicitud para actualizar el uso permitido para igualar dicha cantidad.

60 La Figura 13 es un diagrama de flujo que ilustra operaciones que pueden realizarse mediante un aparato para una función de repositorio de datos configurada para operar en el primer dominio. La función de repositorio de datos puede ser un UDR. El aparato de la Figura 13 puede interactuar con el aparato de la Figura 12.

65

En 1301, el aparato almacena información de suscripción para un abonado, en donde el abonado está suscrito en un dominio diferente al dominio en el que está configurada para operar la función de repositorio de datos, comprendiendo la información de suscripción un valor para un uso permitido para el abonado.

5 En 1302, el aparato recibe, desde una primera función de control de políticas configurada para operar en el primer dominio, una solicitud para actualizar el valor para el uso permitido a otro valor. La primera función de control de políticas puede ser la primera función de control de políticas de la Figura 12.

10 En 1303, el aparato actualiza la información de suscripción almacenada cambiando el valor para el uso permitido al otro valor. El otro valor puede ser un uso permitido restante. El uso permitido restante puede ser el que se discute en los ejemplos anteriores.

15 El aparato puede recibir, desde la primera función de control de políticas, una solicitud de al menos uno del valor y el otro valor. En respuesta a esta solicitud, el aparato puede proporcionar el valor solicitado a la primera función de control de políticas.

La Figura 14 es un diagrama de flujo que ilustra operaciones que pueden realizarse mediante un aparato para una función de gestión de sesiones. La función de gestión de sesiones puede configurarse para funcionar en el primer dominio.

20 En 1401, el aparato puede señalar, a una función de gestión de datos configurada para operar en un segundo dominio, una solicitud de información de suscripción para un abonado, en donde el abonado está suscrito en el segundo dominio y la función de gestión de sesiones está configurada para operar en un primer dominio.

25 En 1402, el aparato recibe, desde la función de gestión de datos, un uso permitido para el abonado.

30 En 1403, el aparato señala una solicitud de una política para una sesión para el abonado a una primera función de control de políticas configurada para operar en el mismo dominio que la función de gestión de sesiones, comprendiendo la solicitud el uso permitido. La primera función de control de políticas puede ser la primera función de control de políticas de la Figura 12.

En 1404, el aparato recibe dicha política desde la primera función de control de políticas.

35 La Figura 15 es un diagrama de flujo que ilustra operaciones potenciales que pueden realizarse mediante un aparato para una función de gestión de datos configurada para operar en un segundo dominio.

40 En 1501, el aparato recibe, desde una función de gestión de sesiones configurada para operar en el primer dominio, una solicitud de información de suscripción para un abonado suscrito en el segundo dominio. La función de gestión de sesiones puede ser el aparato de la Figura 14.

45 En 1502, el aparato señala la información de suscripción almacenada a la función de gestión de sesiones, comprendiendo la información de suscripción almacenada una indicación de un uso permitido para el abonado.

En todos los ejemplos anteriores de las Figuras 12 a 15, el primer dominio puede ser un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.

50 A diferencia de un equivalente 5G de la solución 4G basada en S9 discutida anteriormente, los mecanismos descritos actualmente permiten la activación basada en monitorización de políticas determinadas por la VPLMN. Esto soporta el caso de uso de protección de la red VPLMN de la sobrecarga provocada por los itinerantes. Además, el uso de los mecanismos propuestos puede conducir a reacciones más rápidas y sencillas al alcanzar los límites de uso porque la VPLMN puede reaccionar sin necesidad de ponerse en contacto con la HPLMN. Con respecto a los ejemplos comentados anteriormente, se entiende que son combinados.

55 La figura 2 muestra una realización de ejemplo de un aparato de control para un sistema de comunicación para, por ejemplo, acoplarse a y/o controlar una estación de un sistema de acceso, tal como un nodo RAN, por ejemplo, una estación base, un nodo gNB, una unidad central de una arquitectura en la nube de una red básica tal como una MME o S-GW, una entidad de programación tal como una entidad de gestión de espectro, o un servidor y un anfitrión, por ejemplo, un aparato anfitrión de una NRF, NWDAF, AMF, SMF, un UDM/UDR, etc. El aparato de control puede estar integrado con, o ser externo a, un nodo o módulo de una red de núcleo o RAN. En algunas realizaciones, las estaciones base comprenden una unidad o módulo de aparato de control separado. En otras realizaciones, el aparato de control puede ser otro elemento de red, tal como un controlador de red de radio o un controlador de espectro. El aparato 200 de control se puede disponer para proporcionar control sobre las comunicaciones en el área de servicio del sistema. El aparato 200 comprende al menos una memoria 201, al menos una unidad 202, 203 de procesamiento de datos y una interfaz 204 de entrada/salida. A través de la interfaz, el aparato de control puede acoplarse a un receptor y un transmisor del aparato. El receptor y/o el transmisor pueden implementarse como un extremo frontal de radio o un cabezal de radio remoto. Por ejemplo, el aparato 200 de control o el procesador 201 se puede configurar para ejecutar un código informático apropiado para proporcionar las funciones de control.

Ahora se describirá en mayor detalle un posible dispositivo de comunicación inalámbrica haciendo referencia a la Figura 3, que muestra una vista esquemática parcialmente en sección de un dispositivo 300 de comunicación. Un dispositivo de comunicación de este tipo se denomina a menudo equipo de usuario (UE) o terminal. Cualquier dispositivo que pueda enviar y recibir señales de radio puede proporcionar un dispositivo de comunicación móvil apropiado. Los ejemplos no limitativos comprenden una estación móvil (MS) o un dispositivo móvil, tal como un teléfono móvil o lo que se conoce como un 'teléfono inteligente', un ordenador proporcionado con una tarjeta de interfaz inalámbrica u otra instalación de interfaz inalámbrica (por ejemplo, mochila USB), asistente de datos personales (PDA) o una tableta proporcionada con capacidades de comunicación inalámbrica o cualquier combinación de estos o similares. Un dispositivo de comunicación móvil puede proporcionar, por ejemplo, comunicación de datos para llevar comunicaciones tales como voz, correo electrónico (e-mail), mensajes de texto, multimedia y así sucesivamente. De este modo, a los usuarios se les pueden ofrecer y proporcionar numerosos servicios a través de sus dispositivos de comunicación. Los ejemplos no limitativos de estos servicios comprenden llamadas bidireccionales o multidireccionales, servicios de comunicación de datos o multimedia o simplemente un acceso a un sistema de red de comunicaciones de datos, tal como Internet. Los usuarios también pueden recibir datos de difusión o multidifusión. Los ejemplos no limitativos del contenido comprenden descargas, programas de radio y televisión, vídeos, anuncios, diversas alertas y otra información.

Un dispositivo de comunicación inalámbrica puede ser, por ejemplo, un dispositivo móvil, es decir, un dispositivo que no está atado a una ubicación particular, o puede ser un dispositivo estacionario. El dispositivo inalámbrico puede necesitar una interacción humana para la comunicación o puede no necesitar ninguna interacción humana para la comunicación. En las presentes enseñanzas, los términos UE o "usuario" se emplean para referirse a cualquier tipo de dispositivo de comunicación inalámbrica.

El dispositivo inalámbrico 300 puede recibir señales por una interfaz 307 aérea o de radio a través de un aparato apropiado para la recepción y puede transmitir señales a través de un aparato apropiado para transmitir señales de radio. En la Figura 3, el aparato transceptor está designado esquemáticamente por un bloque 306. El aparato transceptor 306 se puede proporcionar, por ejemplo, por medio de una parte de radio y una disposición de antena asociada. La disposición de antena puede estar dispuesta interna o externamente al dispositivo inalámbrico.

Un dispositivo inalámbrico típicamente está dotado de al menos una entidad 301 de procesamiento de datos, de al menos una memoria 302 y de otros posibles componentes 303 para su uso en la ejecución asistida por software y hardware de las tareas para las que está diseñado para realizar, que incluyen un control de acceso a y comunicaciones con sistemas de acceso y otros dispositivos de comunicación. El procesamiento de datos, el almacenamiento y otros aparatos de control relevantes pueden proporcionarse en una placa de circuito apropiada y/o en conjuntos de chips. Esta característica se denota mediante la referencia 704. El usuario puede controlar el funcionamiento del dispositivo inalámbrico por medio de una interfaz de usuario adecuada, tal como un teclado numérico 305, comandos de voz, un panel o pantalla táctil, combinaciones de los mismos o interfaces similares. También se pueden proporcionar un monitor 308, un altavoz y un micrófono. Además, un dispositivo de comunicación inalámbrica puede comprender unos conectores apropiados (o bien cableados o bien inalámbricos) a otros dispositivos y/o para conectar accesorios externos, por ejemplo, un equipo de manos libres, al mismo.

La Figura 4 muestra una representación esquemática de medios de memoria no volátiles 400a (p. ej., disco de ordenador (CD) o disco versátil digital (DVD)) y 400b (por ejemplo, barra de memoria de bus serie universal (USB)) que almacena instrucciones y/o parámetros 402 que cuando son ejecutados por un procesador permiten que el procesador realice una o más de las etapas de los métodos de la Figura 12 y/o la Figura 13 y/o la Figura 14 y/o la Figura 15.

Por lo tanto, las realizaciones pueden variar dentro del alcance de las reivindicaciones adjuntas. En general, algunas realizaciones pueden implementarse en hardware o circuitos de propósito especial, software, lógica o cualquier combinación de los mismos. Por ejemplo, algunos aspectos pueden implementarse en hardware, mientras que otros aspectos pueden implementarse en firmware o software que puede ejecutarse mediante un controlador, microprocesador u otro dispositivo informático, aunque las realizaciones no se limitan a los mismos. Si bien se pueden ilustrar y describir diversas realizaciones como diagramas de bloques, diagramas de flujo o utilizando alguna otra representación pictórica, se entiende bien que estos bloques, aparatos, sistemas, técnicas o métodos descritos en la presente memoria se pueden implementar, como ejemplos no limitantes, hardware, software, firmware, circuitos o lógica de propósito especial, hardware o controlador de propósito general u otros dispositivos informáticos, o alguna combinación de los mismos.

Las realizaciones pueden implementarse mediante software informático almacenado en una memoria y ejecutable por al menos un procesador de datos de las entidades involucradas o por hardware, o mediante una combinación de software y hardware. Además, en este sentido, cabe señalar que cualesquiera procedimientos, es decir, como en la Figura 12 y/o la Figura 13 y/o la Figura 14 y/o la Figura 15, pueden representar etapas del programa, o circuitos lógicos interconectados, bloques y funciones, o una combinación de etapas de programa y circuitos lógicos, bloques y funciones. El software puede almacenarse en medios físicos tales como chips de memoria, o bloques de memoria implementados dentro del procesador, medios magnéticos tales como disco duro o disquetes, y medios ópticos tales como, por ejemplo, DVD y sus variantes de datos, CD.

La memoria puede ser de cualquier tipo adecuado para el entorno técnico local y puede implementarse usando cualquier tecnología de almacenamiento de datos adecuada, tal como dispositivos de memoria basados en semiconductores, dispositivos y sistemas de memoria magnéticos, dispositivos y sistemas de memoria ópticos, memoria fija y memoria extraíble. Los procesadores de datos pueden ser de cualquier tipo adecuado para el entorno técnico local, y pueden incluir uno o más de ordenadores de propósito general, ordenadores de propósito especial, microprocesadores, digital signal processors (procesadores de señales digitales, DSP), circuitos integrados específicos de aplicación (AStudy ItemC), circuitos de nivel de puerta y procesadores basados en arquitectura de procesador de múltiples núcleos, como ejemplos no limitativos.

Alternativa o adicionalmente, algunas realizaciones pueden implementarse usando circuitería. La circuitería puede configurarse para realizar una o más de las funciones y/o pasos del método descritas anteriormente. Esa circuitería puede proporcionarse en la estación base y/o en el dispositivo de comunicaciones.

Tal y como se emplea en esta solicitud, el término “circuitería” puede referirse a uno o a más o a todos de los siguientes conceptos:

(a) implementaciones de circuitos solo en hardware (tales como implementaciones en circuitería solo analógica y/o digital) y

(b) combinaciones de circuitos físicos y software, tales como (según corresponda):

(i) una combinación de circuito(s) de hardware analógico y/o digital con software/firmware y

(ii) cualquier parte de procesador(es) de hardware con software (incluido(s) procesador(es) de señal digital), software y memoria(s) que trabajan juntos para hacer que un aparato, como el dispositivo de comunicaciones o la estación base, realice las diversas funciones previamente descritas; y

(c) un(os) circuito(s) de hardware y/o procesador(es), tales como un(os) microprocesador(es) o parte de un(os) microprocesador(es), que requiere(n) un software (p. ej., firmware) para su funcionamiento, pero el software puede no estar presente cuando no sea necesario para el funcionamiento.

Esta definición de circuitería aplica a todos los usos de este término en esta solicitud, incluyendo en cualquier reivindicación. Como ejemplo adicional, tal y como se emplea en esta solicitud, el término circuitería también cubre una implementación de tan solo un circuito físico o un procesador (o múltiples procesadores) o de una parte de un circuito físico o de un procesador y de su software y/o firmware acompañante. El término circuitería también cubre, por ejemplo, un dispositivo integrado.

La descripción anterior ha proporcionado a modo de ejemplos ejemplares y no limitativos una descripción completa e informativa de algunas realizaciones. Sin embargo, diversas modificaciones y adaptaciones pueden resultar evidentes para los expertos en las técnicas relevantes a la vista de la descripción anterior, cuando se lee junto con los dibujos adjuntos y las reivindicaciones adjuntas. Sin embargo, todas estas modificaciones y similares de las enseñanzas seguirán estando dentro del alcance definido en las reivindicaciones adjuntas.

En lo anterior, se describen diferentes ejemplos usando, como ejemplo de una arquitectura de acceso a la que pueden aplicarse las técnicas descritas en la presente memoria, una arquitectura de acceso de radio basada en evolución a largo plazo avanzada (LTE avanzada, LTE-A) o nueva radio (NR, 5G), sin restringir los ejemplos a una arquitectura de este tipo, sin embargo. Los ejemplos también pueden aplicarse a otros tipos de redes de comunicaciones que tienen medios adecuados mediante el ajuste de parámetros y procedimientos de manera adecuada. Algunos ejemplos de otras opciones para sistemas adecuados son la red de acceso de radio de sistema de telecomunicaciones móviles universal (UMTS) (UTRAN), red de área local inalámbrica (WLAN o Wi-Fi), interoperabilidad mundial para acceso por microondas (WiMAX), Bluetooth®, servicios de comunicaciones personales (PCS), ZigBee®, acceso múltiple por división de código de banda ancha (WCDMA), sistemas que usan tecnología de banda ultra ancha (UWB), redes de sensores, redes ad hoc móviles (MANE) y subsistemas multimedia de protocolo de Internet (IMS) o cualquier combinación de los mismos.

La Figura 5 ilustra ejemplos de arquitecturas de sistema simplificadas que solo muestran algunos elementos y algunas entidades funcionales, siendo todos ellos unidades lógicas cuya implementación puede diferir de lo que se muestra. Las conexiones mostradas en la Figura 5 son conexiones lógicas; las conexiones físicas reales pueden ser diferentes. Es evidente para una persona experta en la técnica que el sistema típicamente comprende también otras funciones y estructuras que las mostradas en la Figura 5.

Sin embargo, los ejemplos no están restringidos al sistema que se proporciona como un ejemplo, sino que una persona experta en la técnica puede aplicar la solución a otros sistemas de comunicación proporcionados con las propiedades necesarias.

El ejemplo de la Figura 5 muestra una parte de una red de acceso por radio ilustrativa. Por ejemplo, la red de acceso por radio puede soportar comunicaciones de enlace lateral que se describen a continuación en mayor detalle.

La Figura 5 muestra los dispositivos 500 y 502. Los dispositivos 500 y 502 están configurados para estar en una conexión inalámbrica en uno o más canales de comunicación con un nodo 504. El nodo 504 está, además, conectado a una red de núcleo 506. En un ejemplo, el nodo 504 puede ser un nodo de acceso, tal como (e/g)NodoB que da servicio a dispositivos en una célula. En un ejemplo, el nodo 504 puede ser un nodo de acceso que no sea 3GPP. El enlace físico desde un dispositivo a un (e/g)NodoB se denomina enlace ascendente o enlace inverso y el enlace físico desde el (e/g)NodoB al dispositivo se denomina enlace descendente o enlace directo. Debe apreciarse que (e/g) los NodoB o sus funcionalidades pueden implementarse usando cualquier nodo, servidor, servidor o punto de acceso, etc., entidad adecuada para tal uso.

Un sistema de comunicación típicamente comprende más de un (e/g)NodoB, en cuyo caso los (e/g)NodoB también pueden configurarse para comunicarse entre sí a través de enlaces, cableados o inalámbricos, diseñados para este propósito. Estos enlaces se pueden usar con fines de señalización. El (e/g) NodoB es un dispositivo informático configurado para controlar los recursos de radio del sistema de comunicación al que está acoplado. El NodoB también puede denominarse estación base, punto de acceso o cualquier otro tipo de dispositivo de interfaz, incluida una estación de retransmisión capaz de operar en un entorno inalámbrico. El (e/g) NodoB incluye o está acoplado a transceptores. Desde los transceptores del (e/g)NodoB, se proporciona una conexión a una unidad de antena que establece enlaces de radio bidireccionales con los dispositivos. La unidad de antena puede comprender una pluralidad de antenas o elementos de antena. El (e/g)NodoB está conectado, además, a la red de núcleo 506 (CN o núcleo de próxima generación NGC). Dependiendo de la tecnología implementada, el (e/g)NodoB está conectado a una puerta de enlace de red de datos de paquetes y servicio (S-GW + P-GW) o una función de plano de usuario (UPF) para enrutar y reenviar paquetes de datos de usuario y para proporcionar conectividad de dispositivos a una o más redes de paquetes de datos externas, y a una entidad de gestión móvil (MME) o función de gestión de movilidad de acceso (AMF) para controlar el acceso y la movilidad de los dispositivos.

Algunos ejemplos de un dispositivo son una unidad de abonado, un dispositivo de usuario, un equipo de usuario (UE), un terminal de usuario, un dispositivo terminal, una estación móvil, un dispositivo móvil, etc.

El dispositivo se refiere típicamente a un dispositivo móvil o estático (p. ej., un dispositivo informático portátil o no portátil) que incluye dispositivos de comunicación móviles inalámbricos que funcionan con o sin un módulo de identificación de abonado universal (USIM), incluyendo, pero sin limitarse a, los siguientes tipos de dispositivos: un teléfono móvil, un teléfono inteligente, un asistente digital personal (PDA), un teléfono, un dispositivo que usa un módem inalámbrico (dispositivo de alarma o de medición, etc.), un ordenador portátil y/o de pantalla táctil, una tableta, una consola de videojuegos, un miniordenador portátil y un dispositivo multimedia. Debe apreciarse que un dispositivo también puede ser un dispositivo de sólo enlace ascendente casi exclusivo, de los que un ejemplo es una cámara o videocámara que sube imágenes o segmentos de vídeo a una red. Un dispositivo también puede ser un dispositivo que tenga la capacidad de operar en una red de Internet of Things (Internet de las cosas - IoT), que es un escenario en el que los objetos tienen la capacidad de transferir datos a través de una red sin requerir la interacción de persona a persona o de persona a ordenador, p. ej., para su uso en redes eléctricas inteligentes y vehículos conectados. El dispositivo también puede utilizar la nube. En algunas aplicaciones, un dispositivo puede comprender un dispositivo portátil de usuario con partes de radio (tal como un reloj, auriculares o anteojos) y el cálculo se lleva a cabo en la nube.

El dispositivo ilustra un tipo de aparato al que se asignan y ceden recursos en la interfaz aérea y, por lo tanto, cualquier característica descrita en la presente memoria con un dispositivo puede implementarse con un aparato correspondiente, tal como un nodo de retransmisión. Un ejemplo de un nodo de retransmisión de este tipo es un relé de capa 3 (retransmisión automática) hacia la estación base. El dispositivo (o, en algunos ejemplos, un nodo de retransmisión de capa 3) está configurado para realizar una o más de las funcionalidades del equipo de usuario.

También se pueden aplicar diversas técnicas descritas en la presente memoria a un sistema ciberfísico (CPS) (un sistema de elementos computacionales colaborativos que controlan entidades físicas). Los CPS pueden permitir la implementación y explotación de cantidades masivas de dispositivos de tecnología de la información y las comunicaciones, ICT, interconectados (sensores, actuadores, procesadores, microcontroladores, etc.) integrados en objetos físicos en diferentes ubicaciones. Los sistemas ciberfísicos móviles, en los que el sistema físico en cuestión tiene movilidad inherente, son una subcategoría de sistemas ciberfísicos. Los ejemplos de sistemas físicos móviles incluyen robótica móvil y electrónica transportada por seres humanos o animales.

Además, si bien los aparatos se han representado como entidades únicas, se pueden implementar diferentes unidades, procesadores y/o unidades de memoria (no se muestran todos en la Figura 5).

5G permite el uso de antenas de múltiples entradas y múltiples salidas (MIMO), muchas más estaciones base o nodos que LTE (un denominado concepto de células pequeñas), incluyendo macrositios que operan en cooperación con estaciones más pequeñas y el empleo de una variedad de tecnologías de radio dependiendo de las necesidades del servicio, los casos de uso y/o el espectro disponible. Las comunicaciones móviles 5G soportan una gama amplia de casos de uso y aplicaciones relacionadas, incluida la transmisión de video, la realidad aumentada, diferentes maneras

de compartir datos y diversas formas de aplicaciones tipo máquina (tales como comunicaciones tipo máquina (masivas) (mMTC), incluida la seguridad vehicular, diferentes sensores y control en tiempo real). Se prevé que el 5G tenga múltiples interfaces de radio, p. ej., por debajo de 6 GHz o por encima de 24 GHz, cmOnda y mmOnda, y que también sea integrable con tecnologías de acceso por radio heredadas existentes, tal como LTE. La integración con LTE puede implementarse, al menos en la fase inicial, como un sistema, donde la macrocobertura es proporcionada por LTE y el acceso de interfaz de radio 5G procede de células pequeñas mediante la agregación a LTE. En otras palabras, se planea que 5G soporte tanto la operatividad entre RAT (tal como LTE-5G) como la operatividad entre RI (operabilidad de interfaz entre radios, tal como por debajo de 6 GHz, cmOnda, 6 o por encima de 24 GHz, cmOnda y mmOnda). Uno de los conceptos que se considera utilizado en las redes 5G es el corte de red, donde se pueden crear múltiples subredes virtuales (instancias de red) independientes y dedicadas dentro de la misma infraestructura para ejecutar servicios que tienen diferentes requisitos de latencia, fiabilidad, rendimiento y movilidad.

La arquitectura actual de las redes LTE está completamente distribuida en la radio y completamente centralizada en la red de núcleo. Las aplicaciones y los servicios de baja latencia en 5G requieren un acercamiento del contenido a la radio, lo que conduce a una ruptura local (LBO) y una computación perimetral de acceso múltiple (MEC).

5G permite que la generación de análisis y conocimiento se produzca en la fuente de los datos. Este enfoque requiere el aprovechamiento de recursos que pueden no estar conectados continuamente a una red, tales como ordenadores portátiles, teléfonos inteligentes, tabletas y sensores. MEC proporciona un entorno informático distribuido para alojamiento de aplicaciones y servicios. También tiene la capacidad de almacenar y procesar contenido cerca de los abonados de telefonía móvil para un tiempo de respuesta más rápido. La computación perimetral abarca una amplia gama de tecnologías, tales como redes de sensores inalámbricos, adquisición de datos móviles, análisis de firmas móviles, redes cooperativas distribuidas entre pares *ad hoc* y procesamiento también clasificables como computación en la nube/fog computing local y computación en malla/mesh computing, dew computing, computación perimetral móvil, cloudlet, almacenamiento y recuperación de datos distribuidos, redes autónomas de autorreparación, servicios en la nube remotos, realidad aumentada y virtual, almacenamiento en caché de datos, Internet de las Cosas (conectividad masiva y/o crítica en latencia), comunicaciones críticas (vehículos autónomos, seguridad vial, análisis en tiempo real, control crítico en el tiempo, aplicaciones de salud).

El sistema de comunicación también puede comunicarse con otras redes 5G, tales como una red telefónica pública conmutada, una red VoIP, Internet o una red privada, o utilizar servicios proporcionados por ellas. La red de comunicación también puede ser capaz de soportar el uso de servicios en la nube, por ejemplo, al menos parte de las operaciones de la red de núcleo pueden llevarse a cabo como un servicio en la nube (esto se ilustra en la Figura 5 mediante la “nube” 514). El sistema de comunicación también puede comprender una entidad de control central, o similar, que proporcione instalaciones para que redes de diferentes operadores cooperen, por ejemplo, en la compartición de espectro.

La tecnología de la nube perimetral (Edge Cloud) se puede incorporar a una red de acceso por radio (RAN) mediante la utilización de virtualización de funciones de red (NFV) y redes definidas por software (SDN). El uso de la tecnología de nube perimetral puede significar que las operaciones de nodo de acceso se llevarán a cabo, al menos parcialmente, en un servidor, anfitrión o nodo acoplado operativamente a una estación base o cabezal de radio remoto que comprende partes de radio. También es posible que las operaciones de nodo se distribuyan entre una pluralidad de servidores, nodos o anfitriones. La aplicación de la arquitectura cloudRAN permite que las funciones RAN en tiempo real se lleven a cabo en, o cerca de, un sitio de antena remota (en una unidad distribuida, DU, 508) y funciones en tiempo no real que se lleven a cabo de manera centralizada (en una unidad centralizada, CU, 510).

También debe entenderse que la distribución de tareas entre operaciones de red de núcleo y operaciones de estación base puede diferir de la de la LTE o incluso no existir. Algunos otros avances tecnológicos que probablemente se utilicen son los macrodatos y todo IP, que pueden cambiar la forma en que se construyen y gestionan las redes. Las redes 5G (o nueva radio, NR) se están diseñando para soportar múltiples jerarquías, donde los servidores MEC se pueden ubicar entre el núcleo y la estación base o NodoB (gNB). Cabe destacar que MEC también se puede aplicar en redes 4G.

5G también puede utilizar comunicación satelital para mejorar o complementar la cobertura del servicio 5G, por ejemplo, proporcionando retransmisión. Los posibles casos de uso son proporcionar continuidad del servicio para dispositivos máquina a máquina (M2M) o Internet de las cosas (IoT) o para pasajeros a bordo de vehículos, banda ancha móvil (MBB) o garantizar la disponibilidad del servicio para comunicaciones críticas y comunicaciones ferroviarias/marítimas/aeronáuticas futuras. Las comunicaciones por satélite pueden utilizar sistemas de satélites de órbita terrestre geoestacionaria (GEO), pero también sistemas de satélites de órbita terrestre baja (LEO), en particular, megaconstelaciones (sistemas en los que se despliegan cientos de (nano)satélites). Cada satélite de la megaconstelación puede abarcar varias entidades de red habilitadas para satélites que crean células en tierra. Las células en tierra podrán crearse a través de un nodo de retransmisión en tierra o mediante un gNB ubicado en tierra o en un satélite.

Es evidente para una persona experta en la técnica que el sistema representado es únicamente un ejemplo de una parte de un sistema de acceso por radio y, en la práctica, el sistema puede comprender una pluralidad de (e/g)NodoB, el dispositivo puede tener un acceso a una pluralidad de células de radio y el sistema puede comprender también otros aparatos, tales como nodos de retransmisión de capa física u otros elementos de red, etc. Al menos uno de los

- (e/g)NodoB o puede ser un (e/g)NodoB doméstico. Además, en una zona geográfica de un sistema de comunicación por radio, puede estar provista una pluralidad de tipos diferentes de células de radio, así como una pluralidad de células de radio. Las células de radio pueden ser macrocélulas (o células paraguas), que son células grandes que normalmente tienen un diámetro de hasta decenas de kilómetros, o células más pequeñas, tales como microcélulas, femtocélulas o picocélulas. Los (e/g)NodoB de la Figura 5 pueden proporcionar cualquier tipo de estas células. Un sistema de radio celular puede implementarse como una red multicapa que incluye varios tipos de células. Típicamente, en redes multicapa, un nodo de acceso proporciona un tipo de célula o células y, por lo tanto, se requiere una pluralidad de (e/g)NodoB para proporcionar una estructura de red de este tipo.
- 5
- 10 Para satisfacer la necesidad de mejorar la implementación y el rendimiento de los sistemas de comunicación, se ha introducido el concepto de (e/g)NodoB del tipo “plug-and-play” (listo para usar). Típicamente, una red que es capaz de utilizar (e/g)NodoB del tipo “plug-and-play” (listo para usar), incluye, además de los (e/g)NodoB domésticos (H(e/g)NodoB), una puerta de enlace de NodoB doméstica o HNB-GW (no se muestra en la Figura 5). Una puerta de enlace de HNB (HNB-GW), que típicamente se instala dentro de la red de un operador, puede agregar tráfico de una
- 15 gran cantidad de HNB de regreso a una red de núcleo.

REIVINDICACIONES

1. Un aparato para una primera función de control de políticas, comprendiendo el aparato medios para:
- 5 recibir (1201), desde una función de gestión de sesiones, una solicitud para que se establezca una política para una sesión para un abonado, en donde el abonado está suscrito en un segundo dominio y la primera función de control de políticas está configurada para operar en un primer dominio; determinar (1202) una política para la sesión solicitada, comprendiendo la política determinada una indicación de un uso permitido para el abonado y al menos una condición de activación para que la política se actualice;
- 10 señalar (1203) la al menos una condición de activación a la función de gestión de sesiones; y monitorizar (1204) el uso permitido para el abonado actualizando la política en respuesta a la recepción de una indicación de que se ha cumplido al menos una condición de activación, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 15
2. Un aparato según la reivindicación 1, en donde los medios para determinar una política comprenden medios para:
- 20 señalar, a una segunda función de control de políticas que opera en el segundo dominio, una solicitud para el uso permitido, comprendiendo la solicitud una identificación del abonado y una identificación de la conectividad de datos que se solicita; y recibir el uso permitido desde la segunda función de control de políticas.
3. Un aparato según la reivindicación 2, comprendiendo el aparato medios para:
- 25 señalar, a una función de repositorio de datos configurada para operar en el primer dominio, una solicitud para el uso permitido; y recibir una indicación desde la función de repositorio de datos de que el uso permitido no está disponible en el repositorio de datos;
- 30 en donde dicha señalización a la segunda función de control de políticas se realiza en respuesta a la indicación recibida desde la función de repositorio de datos.
4. Un aparato según cualquiera de las reivindicaciones 2 a 3, en donde la identificación de la conectividad de datos que se solicita comprende una indicación de un nombre de red de datos y una indicación de información de segmento asociada con la sesión que se proporciona.
- 35
5. Un aparato según la reivindicación 1, en donde los medios para determinar una política comprenden medios para:
- 40 señalar, a una función de repositorio de datos que opera en el primer dominio, una solicitud de una cantidad restante del uso permitido, comprendiendo la solicitud una identificación del abonado; y recibir una indicación del uso permitido desde la función de repositorio de datos.
6. Un aparato según la reivindicación 1, en donde la solicitud de una política para que se establezca una sesión para un abonado comprende la indicación del uso permitido.
- 45
7. Un aparato según cualquiera de las reivindicaciones anteriores, en donde dichos medios de monitorización comprenden medios para:
- 50 recibir, desde la función de gestión de sesiones, una indicación de que se ha cumplido al menos una condición de activación; y señalar, a una función de repositorio de datos configurada para operar en el mismo dominio que la primera función de control de políticas, una solicitud para actualizar una información de uso para el abonado que se almacena mediante la función de repositorio de datos.
- 55
8. Un aparato según la reivindicación 7, en donde dichos medios de monitorización comprenden medios para:
- 60 en respuesta a recibir dicha indicación de que se ha cumplido al menos una condición de activación, recuperar información que identifica una cantidad del uso permitido que resta después de que se cumpla la condición de activación, en donde dicha señalización de la solicitud para actualizar la política comprende una solicitud para actualizar el uso permitido.
9. Un aparato para una función de repositorio de datos configurada para operar en un primer dominio, comprendiendo el aparato medios para:
- 65

- almacenar (1301) información de suscripción para un abonado, en donde el abonado está suscrito en un segundo dominio, comprendiendo la información de suscripción un valor para un uso permitido para el abonado;
- 5 recibir (1302), desde una primera función de control de políticas configurada para operar en el primer dominio, una solicitud para actualizar el valor para el uso permitido a otro valor; y actualizar (1303) la información de suscripción almacenada cambiando el valor para el uso permitido a otro valor, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 10 10. Un aparato según la reivindicación 9, comprendiendo el aparato medios para:
- recibir, desde la primera función de control de políticas, una solicitud de al menos uno del valor y el otro valor; y proporcionar el valor solicitado a la primera función de control de políticas.
- 15 11. Un aparato para una función de gestión de sesiones, comprendiendo el aparato medios para:
- 20 señalar (1401), a una función de gestión de datos configurada para operar en un segundo dominio, una solicitud de información de suscripción para un abonado, en donde el abonado está suscrito en el segundo dominio y la función de gestión de sesiones está configurada para operar en un primer dominio;
- recibir (1402), desde la función de gestión de datos, un uso permitido para el abonado;
- 25 señalar (1403) una solicitud de una política para una sesión para el abonado a una primera función de control de políticas configurada para operar en el mismo dominio que la función de gestión de sesiones, comprendiendo la solicitud el uso permitido; y recibir (1404) dicha política desde la primera función de control de políticas, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 30 12. Un aparato para una función de gestión de datos configurada para operar en un segundo dominio, comprendiendo el aparato medios para:
- recibir (1501), desde una función de gestión de sesiones configurada para operar en un primer dominio, una solicitud de información de suscripción para un abonado suscrito en el segundo dominio; y
- 35 señalar (1502) la información de suscripción almacenada a la función de gestión de sesiones, comprendiendo la información de suscripción almacenada una indicación de un uso permitido para el abonado, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 40 13. Un método para un aparato para una primera función de control de políticas, comprendiendo el método:
- recibir (1201), desde una función de gestión de sesiones, una solicitud para que se establezca una política para una sesión para un abonado, en donde el abonado está suscrito en un segundo dominio y la primera función de control de políticas está configurada para operar en un primer dominio;
- 45 determinar (1202) una política para la sesión solicitada, comprendiendo la política determinada una indicación de un uso permitido para el abonado y al menos una condición de activación para que la política se actualice;
- señalar (1203) la al menos una condición de activación a la función de gestión de sesiones; y monitorizar (1204) el uso permitido para el abonado actualizando la política en respuesta a la
- 50 recepción de una indicación de que se ha cumplido al menos una condición de activación, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 55 14. Un método para un aparato para una función de repositorio de datos configurada para operar en un primer dominio, comprendiendo el método:
- almacenar (1301) información de suscripción para un abonado, en donde el abonado está suscrito en un segundo dominio, comprendiendo la información de suscripción un valor para un uso permitido para el abonado;
- 60 recibir (1302), desde una primera función de control de políticas configurada para operar en el primer dominio, una solicitud para actualizar el valor para el uso permitido a otro valor; y actualizar (1303) la información de suscripción almacenada cambiando el valor para el uso permitido a otro valor, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 65 15. Un método para un aparato para una función de gestión de sesiones, comprendiendo el método:

- 5 señalizar (1401), a una función de gestión de datos configurada para operar en un segundo dominio, una solicitud de información de suscripción para un abonado, en donde el abonado está suscrito en el segundo dominio y la función de gestión de sesiones está configurada para operar en un primer dominio;
- recibir (1402), desde la función de gestión de datos, un uso permitido para el abonado;
- señalizar (1403) una solicitud de una política para una sesión para el abonado a una primera función de control de políticas configurada para operar en el mismo dominio que la función de gestión de sesiones, comprendiendo la solicitud el uso permitido; y
- 10 recibir (1404) dicha política desde la primera función de control de políticas, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
16. Un método para un aparato para una función de gestión de datos configurada para operar en un segundo dominio, comprendiendo el método:
- 15 recibir (1501), desde una función de gestión de sesiones configurada para operar en un primer dominio, una solicitud de información de suscripción para un abonado suscrito en el segundo dominio; y
- señalizar (1502) la información de suscripción almacenada a la función de gestión de sesiones, comprendiendo la información de suscripción almacenada una indicación de un uso permitido para el abonado, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 20
17. Un producto de programa informático que, cuando se ejecuta en un aparato para una primera función de control de políticas, hace que el aparato realice lo siguiente:
- 25 recibir (1201), desde una función de gestión de sesiones, una solicitud para que se establezca una política para una sesión para un abonado, en donde el abonado está suscrito en un segundo dominio y la primera función de control de políticas está configurada para operar en un primer dominio;
- 30 determinar (1202) una política para la sesión solicitada, comprendiendo la política determinada una indicación de un uso permitido para el abonado y al menos una condición de activación para que la política se actualice;
- señalizar (1203) la al menos una condición de activación a la función de gestión de sesiones; y
- 35 monitorizar (1204) el uso permitido para el abonado actualizando la política en respuesta a la recepción de una indicación de que se ha cumplido al menos una condición de activación, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 40
18. Un producto de programa informático que, cuando se ejecuta en un aparato para una función de repositorio de datos configurada para operar en un primer dominio, hace que el aparato realice lo siguiente:
- 45 almacenar (1301) información de suscripción para un abonado, en donde el abonado está suscrito en un segundo dominio, comprendiendo la información de suscripción un valor para un uso permitido para el abonado;
- recibir (1302), desde una primera función de control de políticas configurada para operar en el primer dominio, una solicitud para actualizar el valor para el uso permitido a otro valor; y
- actualizar (1303) la información de suscripción almacenada cambiando el valor para el uso permitido a otro valor, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 50
19. Un producto de programa informático que, cuando se ejecuta en un aparato para una función de gestión de sesiones, hace que el aparato realice lo siguiente:
- 55 señalizar (1401), a una función de gestión de datos configurada para operar en un segundo dominio, una solicitud de información de suscripción para un abonado, en donde el abonado está suscrito en el segundo dominio y la función de gestión de sesiones está configurada para operar en un primer dominio;
- recibir (1402), desde la función de gestión de datos, un uso permitido para el abonado;
- señalizar (1403) una solicitud de una política para una sesión para el abonado a una primera función de control de políticas configurada para operar en el mismo dominio que la función de gestión de sesiones, comprendiendo la solicitud el uso permitido; y
- 60 recibir (1404) dicha política desde la primera función de control de políticas, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.
- 65 20. Un producto de programa informático que, cuando se ejecuta en un aparato para una función de gestión de datos configurada para operar en un segundo dominio, hace que el aparato realice lo siguiente:

- 5 recibir (1501), desde una función de gestión de sesiones configurada para operar en un primer dominio, una solicitud de información de suscripción para un abonado suscrito en el segundo dominio; y
- señalar (1502) la información de suscripción almacenada a la función de gestión de sesiones, comprendiendo la información de suscripción almacenada una indicación de un uso permitido para el abonado, en donde el primer dominio es un dominio visitado y el segundo dominio es un dominio doméstico para el abonado.

Figura 1A

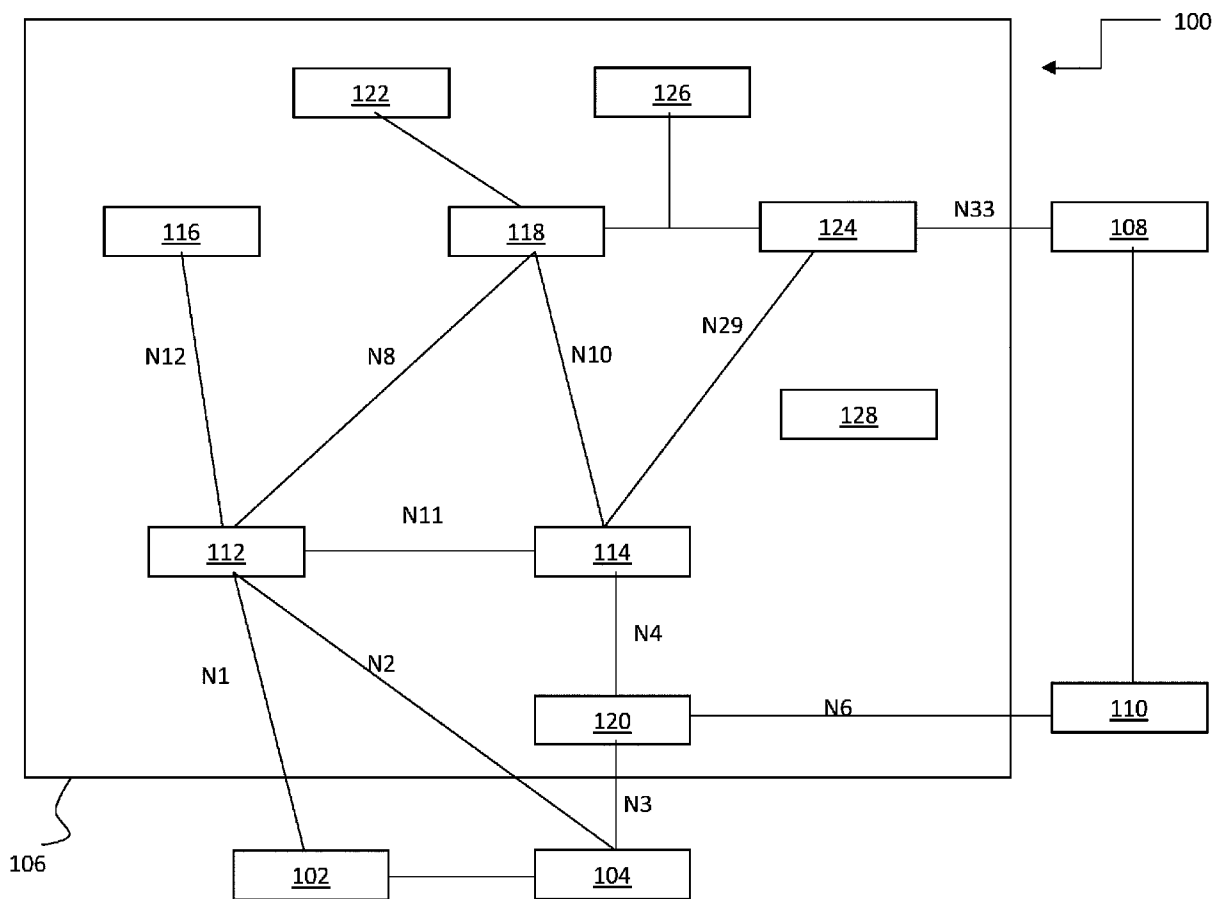
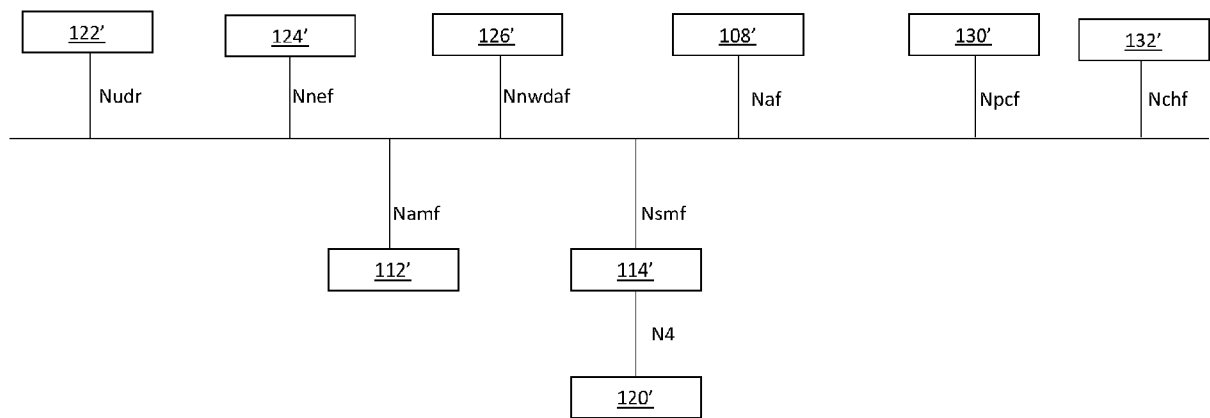


Figura 1B

100



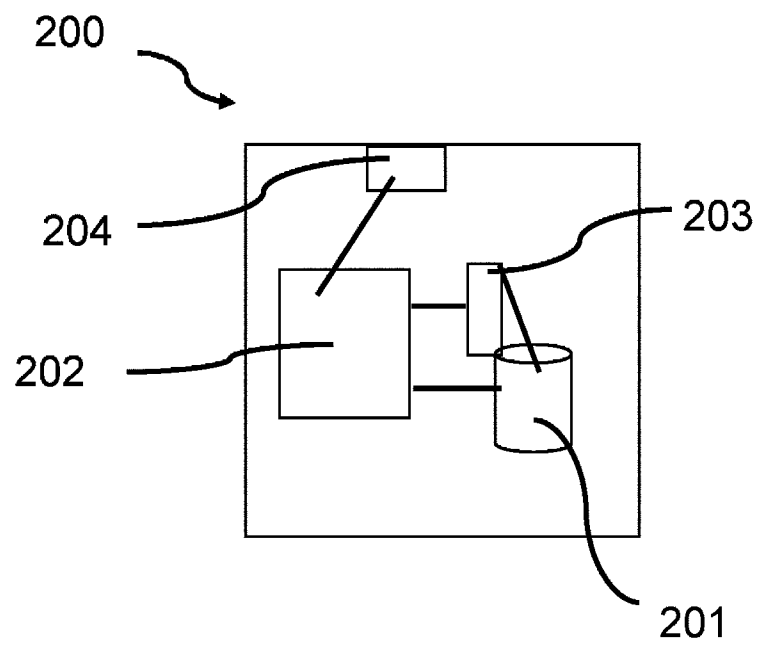


Figura 2

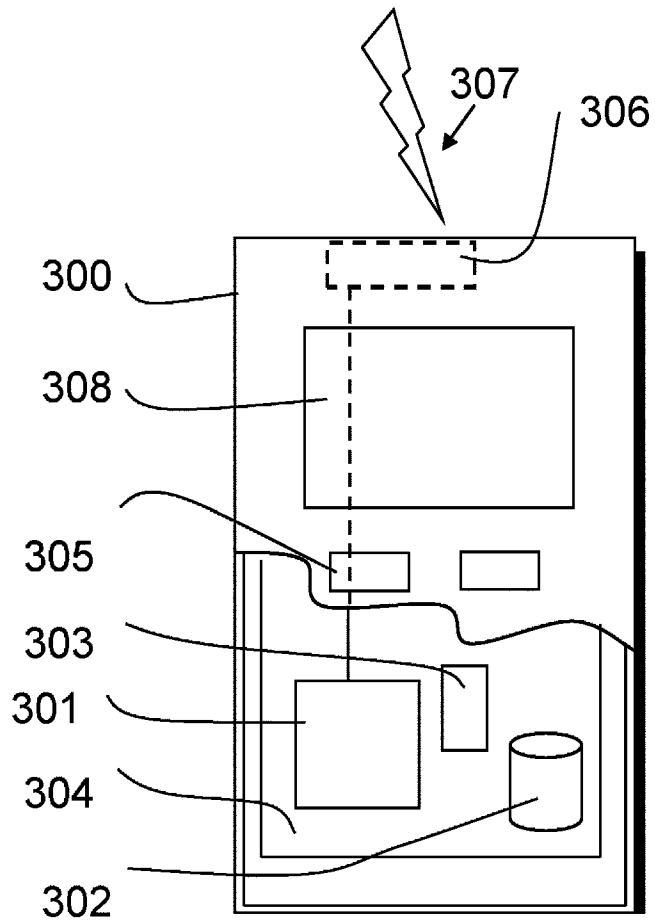


Figura 3

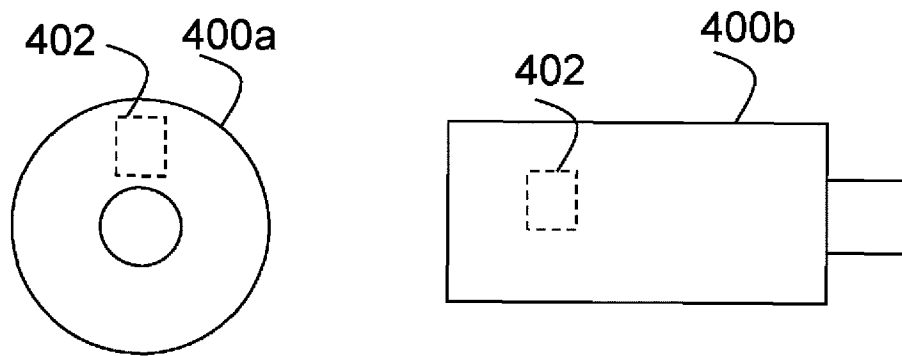
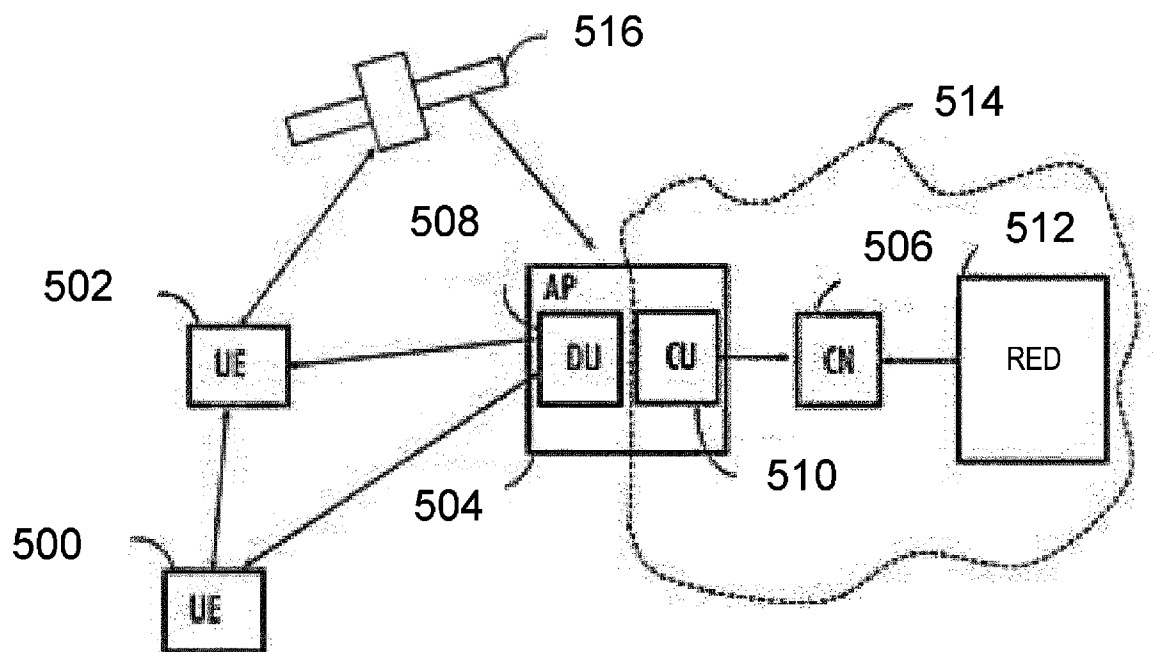


Figura 4

Figura 5



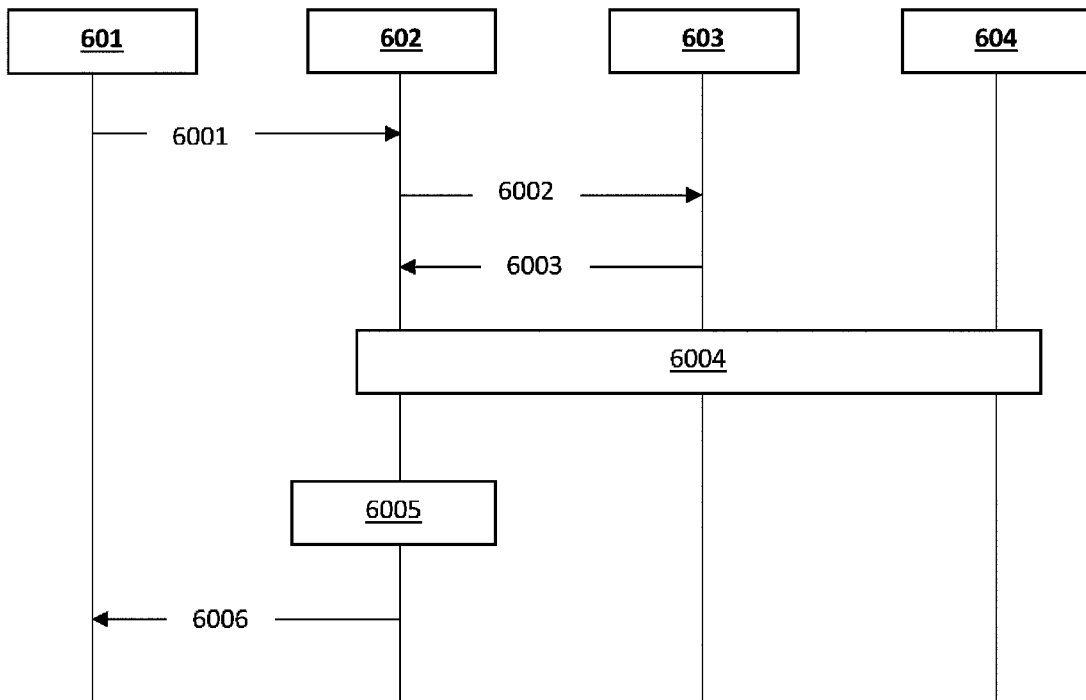


Figura 6

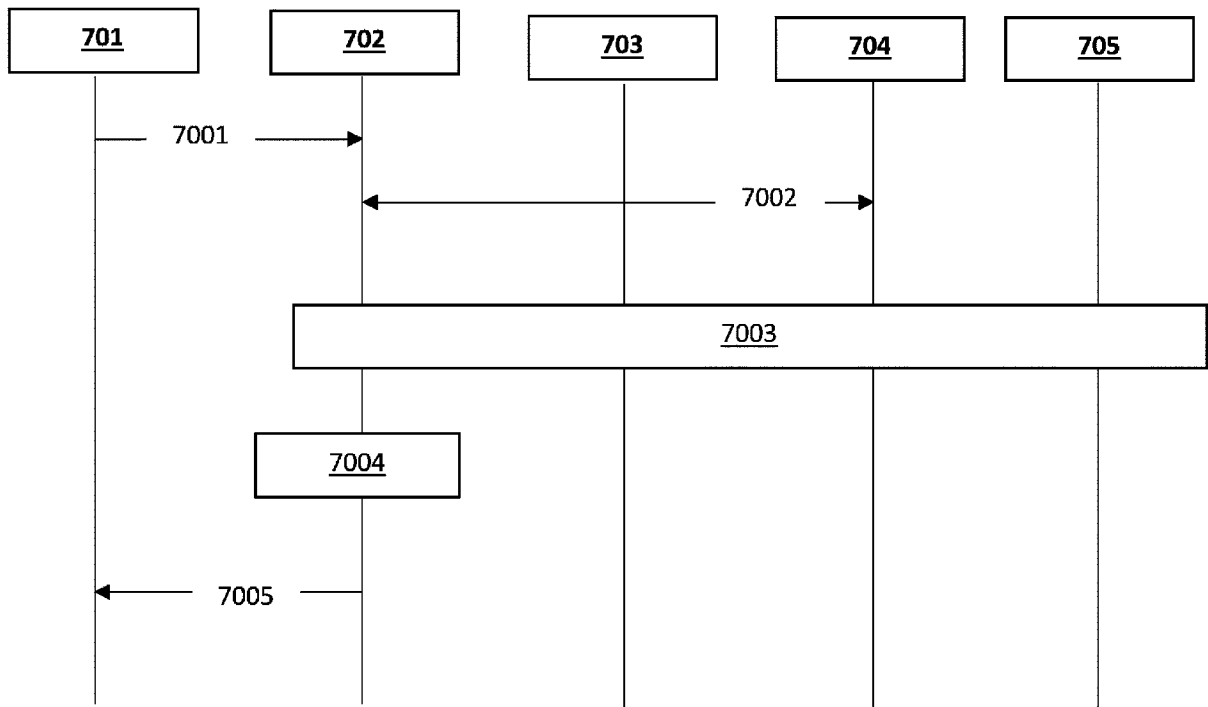


Figura 7

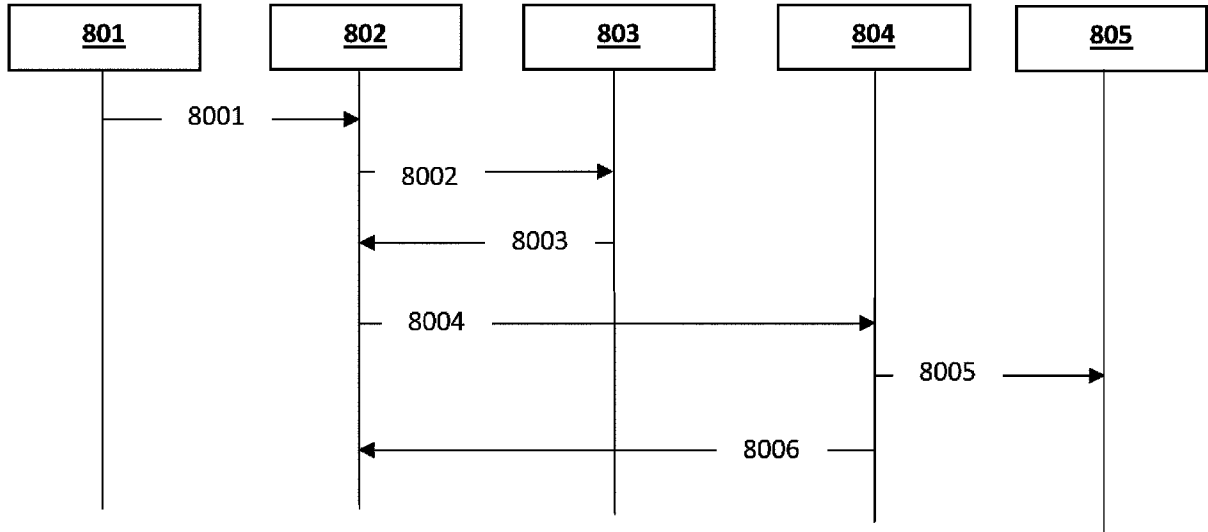


Figura 8

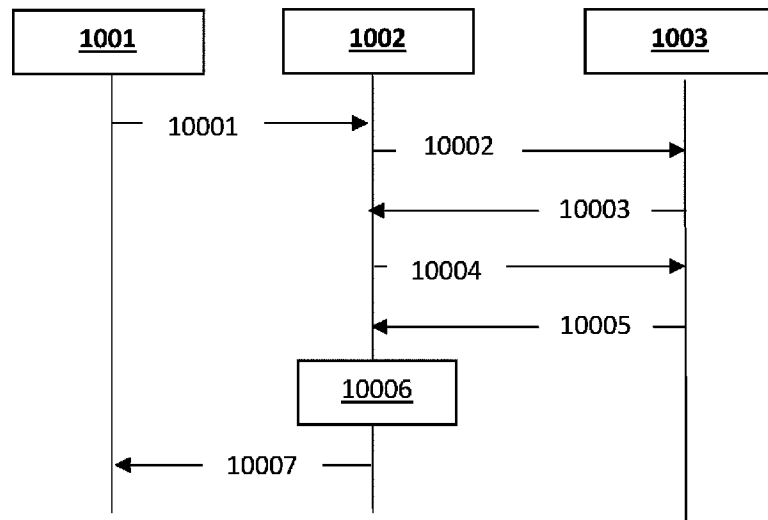


Figura 10

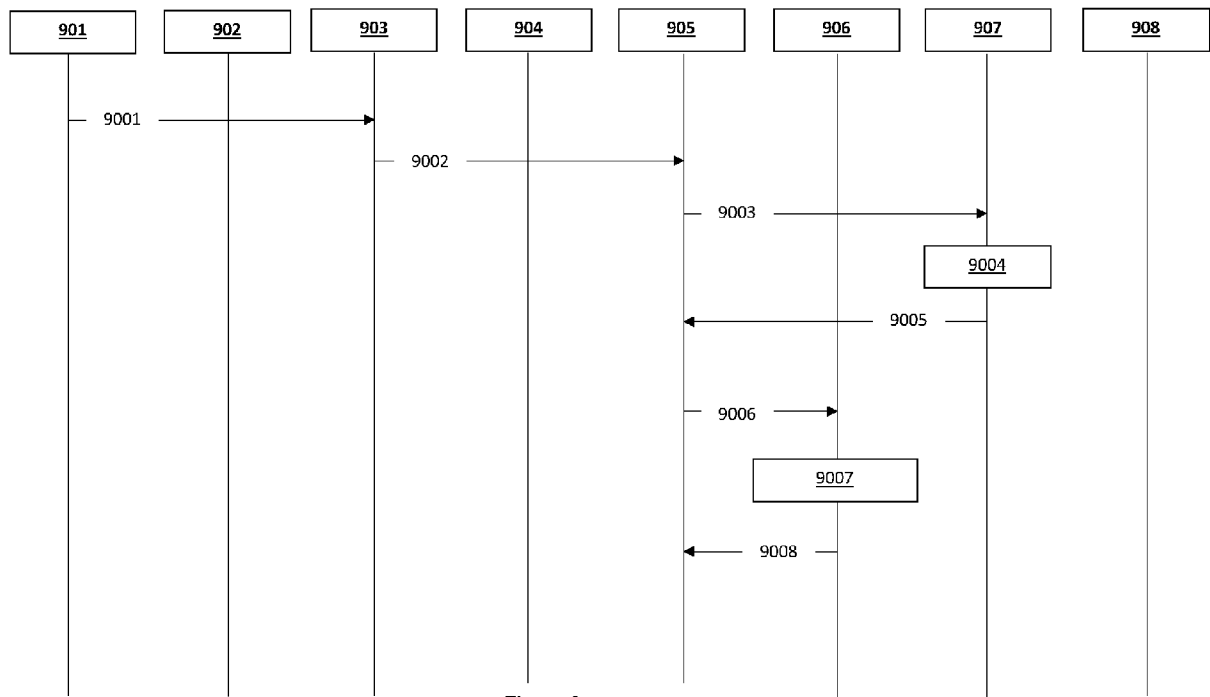


Figura 9

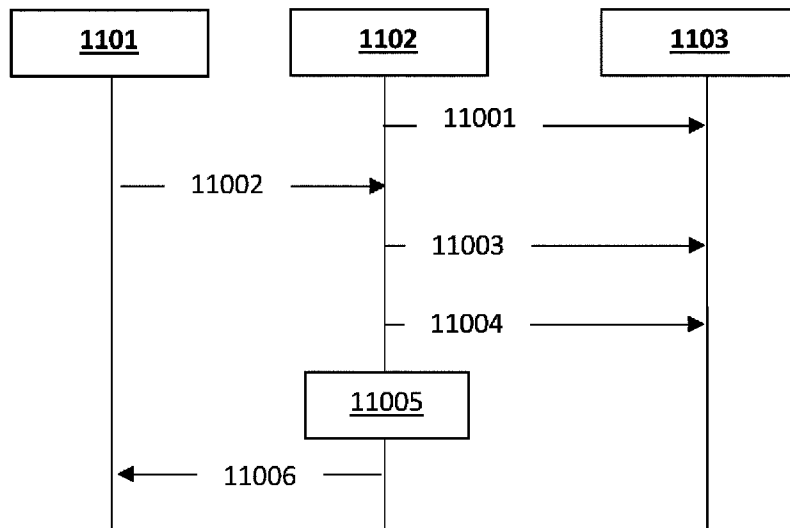


Figura 11

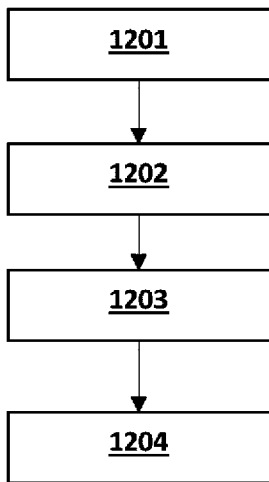


Figura 12

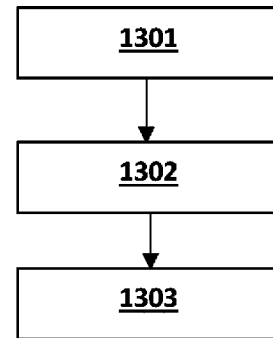


Figura 13

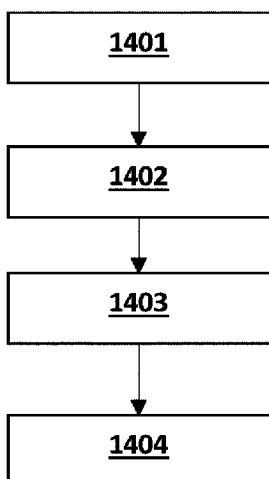


Figura 14

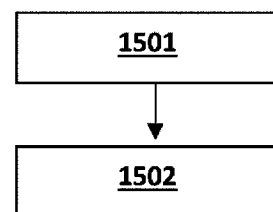


Figura 15