(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 633 107**

(51) Int. CI.:

H04W 48/08 (2009.01)
H04L 29/06 (2006.01)
H04W 12/08 (2009.01)
H04W 8/26 (2009.01)
H04W 12/06 (2009.01)
H04W 48/02 (2009.01)
H04W 48/14 (2009.01)
H04W 84/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.10.2008 PCT/US2008/079113**

(87) Fecha y número de publicación internacional: **16.04.2009 WO09048888**

(96) Fecha de presentación y número de la solicitud europea: **07.10.2008 E 08837923 (5)**

(97) Fecha y número de publicación de la concesión europea: **12.04.2017 EP 2198585**

(54) Título: **Dotación de nodos de comunicación**

(30) Prioridad:

08.10.2007 US 978363 P
01.02.2008 US 25686 P
13.06.2008 US 61537 P
06.10.2008 US 246388

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.09.2017

(73) Titular/es:

QUALCOMM INCORPORATED
5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121, US

(72) Inventor/es:

GUPTA, RAJARSHI;
PALANIGOUNDER, ANAND;
ULUPINAR, FATIH;
HORN, GAVIN B.;
AGASHE, PARAG A.;
CHEN, JEN MEI;
DESHPANDE, MANOJ M.;
BALASUBRAMANIAN, SRINIVASAN;
NANDA, SANJIV y
SONG, OSOK

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Dotación de nodos de comunicación

ANTECEDENTES

Campo

Esta solicitud se refiere, en general, a la comunicación inalámbrica y, más específicamente, aunque no exclusivamente, a mejorar el rendimiento de la comunicación.

Introducción

Los sistemas de comunicación inalámbrica se utilizan ampliamente para proporcionar varios tipos de comunicación (por ejemplo, voz, datos, servicios multimedia, etc.) a múltiples usuarios. Según crece rápidamente la demanda de servicios de datos de multimedios y de alta velocidad, supone un desafío implementar sistemas de comunicación eficientes y robustos con un rendimiento mejorado.

Para complementar las estaciones base de red de telefonía móvil convencionales, pueden desplegarse estaciones base de pequeña cobertura (por ejemplo, instaladas en la casa de un usuario). En algunos aspectos, estas estaciones base pueden proporcionar una cobertura inalámbrica interior más robusta para las unidades móviles. Tales estaciones base de pequeña cobertura se conocen generalmente como estaciones base de punto de acceso, Nodos B domésticos o femto-células. Normalmente, tales estaciones base de pequeña cobertura están conectadas a Internet y a la red del operador móvil mediante un encaminador de DSL o un módem por cable.

La patente estadounidense Nº 7.263.076 (Leibovitz y col.) describe un sistema de gestión comunitario que incluye un servidor web que interactúa con los propietarios y permite que cada uno de los propietarios se registre como miembro de la comunidad de red. El sistema de gestión comunitario también incluye un servidor de autenticación. La publicación de la patente europea N° 1667358 (Swisscom AG) describe un procedimiento para la configuración dinámica de una subred en la que se configura una frecuencia portadora adicional en un punto de acceso dado. Un punto de acceso dado está configurado por un módulo de configuración de acceso de tal manera que solo se puede acceder al punto de acceso dado de la frecuencia portadora adicional con una identificación de red correspondiente.

MOTOROLA: "Asignación de identidad SCH de células CSG" describe células CSG identificadas por identidades SCH.

VODAFONE Y COL.: «El concepto de célula doméstica del sistema de paquetes mejorado» describe las células CSG identificadas mediante el seguimiento de los códigos de zona y los ID de celda.

NIT DOCOMO Y COL.: "Asignación de ID de célula para el nodo B doméstico" describe células CSG identificadas por ID de celdas.

En algunos escenarios, las estaciones base de pequeña cobertura pueden desplegarse según se necesiten. En consecuencia, puede haber problemas asociados al acceso a estas estaciones base. Por ejemplo, tal vez sea necesario configurar los terminales de acceso para acceder a sus estaciones base asociadas. Además, puede ser deseable evitar que los terminales de acceso no autorizados accedan a ciertas estaciones base. Por lo tanto, hay una necesidad de una gestión de acceso mejorada para redes inalámbricas.

SUMARIO

La invención se define en las reivindicaciones independientes. Los modos de realización específicos de la invención se definen en las reivindicaciones dependientes. A continuación se ofrece un sumario de aspectos de muestra de la divulgación. Debería entenderse que cualquier referencia al término ‘aspectos’ en el presente documento puede referirse a uno o más aspectos de la divulgación.

La divulgación se refiere en algún aspecto a dotar nodos de comunicación y proporcionar gestión de acceso para la comunicación inalámbrica. Por ejemplo, los identificadores pueden ser asignados a grupos de nodos en los que se pueden utilizar los identificadores para controlar el acceso a los puntos de acceso restringido que proporcionan ciertos servicios solo a conjuntos definidos de terminales de acceso. Aquí, un punto de acceso restringido puede, por ejemplo, proporcionar ciertos servicios (por ejemplo, facturación diferente, servicios adicionales, diferente calidad de servicio) para los terminales de acceso de uno o más usuarios preferidos, pero no para otros usuarios.

En algunos aspectos, la dotación de un nodo puede implicar proporcionar un identificador único para un conjunto de uno o más nodos. Por ejemplo, un identificador único puede ser asignado a uno o más puntos de acceso restringido. Del mismo modo, un identificador único puede ser asignado a un conjunto de terminales de acceso que están autorizados para recibir servicio desde uno o más puntos de acceso restringido. En algunos aspectos, un

identificador temporal puede ser asignado a un terminal de acceso, por lo cual el acceso al nodo puede implicar la correlación del identificador temporal con un identificador permanente para el terminal de acceso.

Mediante la utilización de tales identificadores, se puede lograr un nivel deseado de control de acceso incluso aunque los nodos puedan ser dotados según se necesite. En algunos aspectos, el control de acceso puede ser proporcionado por un punto de acceso restringido. En algunos aspectos, el control de acceso puede ser proporcionado por un nodo de red. En algunos aspectos, el control de acceso puede ser proporcionado por la cooperación de un punto de acceso restringido y un nodo de red.

La divulgación se refiere, en algunos aspectos, a dotar a un nodo de una lista de itinerancia preferida. En algunos aspectos, un nodo puede ser dotado de una lista de itinerancia preferida por omisión, que el nodo puede utilizar para obtener otra lista de itinerancia preferida para acceder a puntos de acceso restringidos. En algunos aspectos, un nodo puede ser dotado de una lista de itinerancia preferida, mediante el uso de una baliza de arranque.

La invención se refiere a un procedimiento de comunicación realizado por un nodo de red como se expone en la reivindicación 1, un nodo de red como se expone en la reivindicación 9, un procedimiento de comunicación realizado por un conjunto de al menos un punto de acceso como se expone en la reivindicación 10 y un conjunto de al menos un punto de acceso como se expone en la reivindicación 13.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Estos y otros aspectos de ejemplo de la divulgación se describirán en la descripción detallada y las reivindicaciones descritas a continuación y en los dibujos adjuntos, en los que:

la FIG. 1 es un diagrama de bloques simplificado de varios aspectos de muestra de un sistema de comunicación;

la FIG. 2 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para dotar nodos de red y proporcionar control de acceso;

la FIG. 3 es un diagrama simplificado de varios componentes de muestra de nodo de red;

la FIG. 4 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para dotar un punto de acceso;

la FIG. 5 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para dotar un terminal de acceso;

la FIG. 6 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para dotar un terminal de acceso;

la FIG. 7 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para proporcionar control de acceso;

la FIG. 8 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para proporcionar control de acceso;

la FIG. 9 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para proporcionar control de acceso;

la FIG. 10 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para proporcionar control de acceso;

la FIG. 11 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para proporcionar control de acceso;

la FIG. 12 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para dotar un terminal de acceso;

la FIG. 13 es un diagrama de flujo de varios aspectos de muestra de operaciones que pueden utilizarse para proporcionar control de acceso;

la FIG. 14 es un diagrama simplificado de un sistema de comunicación inalámbrica;

la FIG. 15 es un diagrama simplificado de un sistema de comunicación inalámbrica que incluye femto-nodos;

la FIG. 16 es un diagrama simplificado que ilustra áreas de cobertura para la comunicación inalámbrica;

la FIG. 17 es un diagrama de bloques simplificado de varios aspectos de muestra de componentes de comunicación;

y las FIGs. 18 a 28 son diagramas de bloques simplificados de varios aspectos de muestra de aparatos configurados para proporcionar dotación y/o gestión de acceso, según se instruye en el presente documento.

Según la práctica habitual, las diversas características ilustradas en los dibujos pueden no estar trazadas a escala. Por consiguiente, las dimensiones de las diversas características pueden ampliarse o reducirse de manera arbitraria para una mayor claridad. Además, algunos de los dibujos pueden estar simplificados para una mayor claridad. Por lo tanto, los dibujos pueden no ilustrar todos los componentes de un aparato dado (por ejemplo, un dispositivo) o de un procedimiento. Finalmente, pueden usarse los mismos números de referencia para denotar las mismas características en toda la extensión de la memoria descriptiva y de las figuras.

DESCRIPCIÓN DETALLADA

A continuación se describen varios aspectos de la divulgación. Resultará evidente que las enseñanzas en el presente documento pueden implementarse de muchas maneras diferentes y que cualquier estructura o función específica, o ambas, divulgadas en el presente documento son simplemente representativas. Basándose en las enseñanzas del presente documento, un experto en la técnica apreciará que un aspecto divulgado en el presente documento puede implementarse independientemente de cualquier otro aspecto, y que dos o más de estos aspectos pueden combinarse de varias maneras. Por ejemplo, un aparato puede implementarse, o un procedimiento puede llevarse a la práctica, usando cualquier número de los aspectos dados a conocer en el presente documento. Además, un aparato de este tipo puede implementarse, o un procedimiento de este tipo puede llevarse a la práctica, usando otra estructura, funcionalidad, o estructura y funcionalidad, además de, o distintas a, los uno o más de los aspectos descritos en el presente documento. Además, un aspecto puede comprender al menos un elemento de una reivindicación.

La FIG. 1 ilustra varios nodos de un sistema de comunicación 100 de muestra (por ejemplo, una parte de una red de comunicación). Con fines ilustrativos, varios aspectos de la divulgación se describirán en el contexto de uno o más nodos de red, puntos de acceso y terminales de acceso que se comunican entre sí. Sin embargo, debería apreciarse que las enseñanzas en el presente documento pueden aplicarse a otros tipos de aparatos o a otros aparatos similares a los que se hace referencia usando otra terminología.

Los puntos de acceso 102 y 104 en el sistema 100 proporcionan uno o más servicios (por ejemplo, conectividad de red) para uno o más terminales inalámbricos (por ejemplo, los terminales de acceso 106 y/o 108) que pueden instalarse dentro de los mismos o que pueden desplazarse por toda un área geográfica asociada. Además, los puntos de acceso 102 y 104 pueden comunicarse con uno o más nodos de red 110 para facilitar la conectividad de red de área amplia. Dicho nodo de red puede adoptar varias formas. Por ejemplo, un nodo de red puede comprender un gestor de movilidad o alguna otra entidad de red adecuada (por ejemplo, una entidad de red central).

Los puntos de acceso 102 y 104 pueden estar restringidos en algunos aspectos, por lo que cada punto de acceso ofrece ciertos servicios a ciertos terminales de acceso (por ejemplo, los terminales de acceso 106 y 108), pero no a otros terminales de acceso (por ejemplo, un macro-terminal de acceso, que no se muestra). Por ejemplo, los puntos de acceso 102 y 104 pueden estar restringidos a no proporcionar, a los otros terminales de acceso, al menos uno entre: registro, señalización, llamada de voz, acceso a datos o cualquier otro servicio celular. Los puntos de acceso restringido pueden desplegarse según se necesiten. Por ejemplo, un propietario doméstico determinado puede instalar y configurar su propio punto de acceso restringido.

La FIG. 2 proporciona una visión general de varias operaciones que pueden llevarse a cabo para facilitar el despliegue de puntos de acceso restringido y los terminales de acceso que están autorizados a utilizar estos puntos de acceso. En algunos aspectos, estas operaciones se pueden utilizar para habilitar un nodo de acceso restringido para determinar su identidad, determinar la identidad de los terminales de acceso a los que se permita acceder (por ejemplo, conectarse) al punto de acceso restringido, y confirmar la identidad de un terminal de acceso (por ejemplo, un terminal de acceso que está intentando acceder al punto de acceso restringido). En algunos aspectos, estas operaciones se pueden utilizar para permitir a un terminal de acceso determinar su identidad, determinar la identidad de un punto de acceso restringido al cual se permita acceder al terminal de acceso, traducir la identidad temporal del terminal de acceso a la identidad permanente del mismo y confirmar la identidad de un punto de acceso (por ejemplo, un punto de acceso restringido al cual esté intentando acceder el terminal de acceso).

Por comodidad, las operaciones de la FIG. 2 (o cualquier otra operación expuesta o enseñada en el presente documento) pueden describirse como llevadas a cabo mediante componentes específicos (por ejemplo, componentes del sistema 100 y/o componentes de un sistema 300 como el mostrado en la FIG. 3). Sin embargo, debería apreciarse que estas operaciones pueden llevarse a cabo mediante otros tipos de componentes y pueden llevarse a cabo usando un número diferente de componentes. También debería apreciarse que una o más de las operaciones descritas en el presente documento pueden no utilizarse en una implementación dada.

La FIG. 3 ilustra varios componentes de muestra que se pueden incorporar en el nodo de red 110 (por ejemplo, un gestor de movilidad, un centro de conmutación móvil o un nodo de soporte del GPRS de servicio), el punto de acceso 102 y el terminal de acceso 106 según las enseñanzas en el presente documento. Se debería apreciar que los componentes ilustrados para un nodo dado de estos nodos también se pueden incorporar en otros nodos en un sistema de comunicación. Por ejemplo, el terminal de acceso 108 puede incluir componentes similares a los descritos para el terminal de acceso 106 y el punto de acceso 104 puede incluir componentes similares a los descritos para el punto de acceso 102.

El nodo de red 110, el punto de acceso 102 y el terminal de acceso 106 incluyen los transceptores respectivos 302, 304 y 306 para comunicarse entre sí y con otros nodos. El transceptor 302 incluye un transmisor 308 para enviar señales (por ejemplo, mensajes) y un receptor 310 para recibir señales. El transceptor 304 incluye un transmisor 312 para transmitir señales y un receptor 314 para recibir señales. El transceptor 306 incluye un transmisor 316 para transmitir señales y un receptor 318 para recibir señales. El nodo de red 110, el punto de acceso 102 y el terminal de acceso 106 también incluyen otros componentes que pueden utilizarse conjuntamente con la dotación de nodos y la gestión de acceso tal como se enseña en el presente documento. Por ejemplo, el nodo de red 110, el punto de acceso 102 y el terminal de acceso 106 pueden incluir los controladores de comunicaciones 320, 322 y 324, respectivamente, para la gestión de las comunicaciones con otros nodos (por ejemplo, enviar y recibir mensajes / indicaciones) y para proporcionar otra funcionalidad relacionada, tal como se enseña en el presente documento. El nodo de red 110, el punto de acceso 102 y el terminal de acceso 106 pueden incluir los controladores de dotación 326, 328 y 330, respectivamente, para la dotación de un nodo y para proporcionar otra funcionalidad relacionada, tal como se enseña en el presente documento. El nodo de red 110, el punto de acceso 102 y el terminal de acceso 106 pueden incluir controladores de acceso 332, 334 y 336, respectivamente, para proporcionar la gestión de acceso y para proporcionar otra funcionalidad relacionada, tal como se enseña en el presente documento. Con fines ilustrativos, todos los nodos se representan en la FIG. 3 como incluyendo funcionalidad relacionada con la dotación y el control de acceso. En algunas implementaciones, sin embargo, uno o más de estos componentes pueden no ser utilizados en un nodo dado. La exposición siguiente describe varios esquemas diferentes (por ejemplo, conjuntamente con diferentes figuras) para dotar a nodos de red y proporcionar control de acceso. Por conveniencia, en estos diferentes esquemas, el nodo de red 110, el punto de acceso 102 y el terminal de acceso 106 pueden ser mencionados como incluyendo diferente funcionalidad y pueden mencionarse como representativos de diferentes tipos de nodos (por ejemplo, en diferentes implementaciones, el nodo de red 110 puede representar un SRNC, o una MME, o un AAA, etc.). Se debería apreciar, sin embargo, que, en una implementación dada, el nodo de red 110, el punto de acceso 102 y el terminal de acceso 106 pueden estar configurados de una manera específica.

Haciendo de nuevo referencia a la FIG. 2, según lo representado mediante el bloque 202, cada terminal de acceso (por ejemplo, el terminal de acceso 106) en un sistema puede ser dotado para permitir la comunicación con uno o más puntos de acceso (por ejemplo, punto de acceso 102). En el ejemplo de la FIG. 3, estas operaciones se pueden realizar, por ejemplo, mediante el funcionamiento de los controladores de dotación 326 y 330.

En algunos aspectos, un operador puede asignar un identificador único al terminal de acceso 106. En algunas implementaciones, este identificador comprende un identificador de acceso a la red ("NAI") o un número de red digital de servicios integrados de estación móvil ("MS ISDN"). Como alternativa, la identidad de abonado, tal como la Identidad de Abonado Móvil Internacional (IMSI), también se puede obtener a partir de un módulo de identidad de abonado, tal como el SIM, el USIM o el VSIM presente en el terminal de acceso. En algunos casos, se garantiza que este identificador sea único dentro de un dominio de operador (por ejemplo, la red completa proporcionada por un operador celular). En algunas implementaciones, un identificador de este tipo puede ser parte de la información de la sesión para el terminal de acceso 106. Por ejemplo, el identificador puede ser enviado al nodo de red 110 (por ejemplo, un controlador de red de referencia de sesión, SRNC) por el terminal de acceso 106 cuando el terminal de acceso 106 crea una sesión, o el identificador puede ser enviado unilateralmente al nodo de red 110 desde una entidad de autentificación, autorización y contabilidad ("AAA") una vez que se crea una sesión. En algunas implementaciones, el identificador es accesible para un usuario, de forma que el usuario pueda, por ejemplo, configurar su(s) punto(s) de acceso restringido para dar servicio a uno o más terminales de acceso. En algunas implementaciones, a un terminal de acceso se le puede asignar un identificador temporal. Por ejemplo, la red puede asignar identificadores permanentes y temporales para el terminal de acceso 106 y mantener esos identificadores en la red. Además, la red puede enviar el identificador temporal al terminal de acceso 106 de modo que el terminal de acceso 106 pueda usar ese identificador cuando acceda a un punto de acceso.

También se puede dotar al terminal de acceso 106 con la identidad de cada punto de acceso (por ejemplo, el punto de acceso 102) al cual se permite el acceso al terminal de acceso 106. Como se describe en más detalle a continuación, esto puede implicar, por ejemplo, el envío de identificadores de punto de acceso al terminal de acceso 106 (por ejemplo, un modelo de envío no solicitado) y/o permitir que el terminal de acceso 106 seleccione los puntos de acceso a los que acceda el terminal de acceso 106 (por ejemplo, un modelo de extracción solicitada). El terminal de acceso 106 puede así mantener una lista de puntos de acceso autorizados (por ejemplo, una lista blanca o lista de zonas de usuario preferidas) a la cual el terminal de acceso 106 puede hacer referencia a medida que se desplaza a través de diferentes áreas de cobertura inalámbrica.

En algunas implementaciones, se puede pedir a un usuario del terminal de acceso 106 que determine si él o ella desea o no habilitar el terminal de acceso 106 para acceder a un punto de acceso. En algunas implementaciones, el terminal de acceso 106 puede habilitar automáticamente el acceso a un punto de acceso. En algunas implementaciones, el terminal de acceso 106 puede determinar, en base a la información de configuración en el terminal de acceso 106, si se habilita automáticamente el acceso o se requiere una solicitud del usuario para permitir el acceso. En algunas implementaciones, un usuario puede elegir acceder o elegir no acceder a uno o más terminales de acceso. En este caso, se puede mantener una lista del (de los) terminal(es) de acceso permitido(s) y/o rechazado(s) en el terminal de acceso 106. De esta manera, el terminal de acceso 106 puede evitar (por ejemplo, evitar automáticamente) el intento de acceder a un punto de acceso en la lista.

Tal como se representa mediante el bloque 204, puede dotarse a cada punto de acceso restringido (por ejemplo, el punto de acceso 102) en un sistema para permitir la comunicación con uno o más terminales de acceso (por ejemplo, el terminal de acceso 106). En el ejemplo de la FIG. 3, estas operaciones se pueden realizar, por ejemplo, mediante el funcionamiento de los controladores de dotación 326 y 328.

Por ejemplo, un identificador único puede ser asignado al punto de acceso 102 o a un conjunto de puntos de acceso (por ejemplo, los puntos de acceso 102 y 104). Este identificador único es diferente a un identificador de dispositivo único que pueda ser asignado para identificar terminales de acceso individuales en un sistema. Como se describe en más detalle a continuación, dicho identificador puede comprender, por ejemplo, un tipo especial de identificador de red ("NID") o identificador de subred, o un identificador asignado a un grupo de terminales de acceso que tengan las mismas propiedades de asociación restringidas (por ejemplo, un CSG). En algunos casos, la red puede asignar un identificador único de manera autónoma. En algunos casos, uno o más puntos de acceso pueden solicitar un identificador (por ejemplo, mediante la determinación de un identificador propuesto y enviándolo a la red). En estos casos, la red puede determinar si el identificador solicitado ya está o no en uso por uno o más puntos de acceso diferentes. Si el identificador solicitado ya está en uso, la red puede seleccionar otro identificador (por ejemplo, un identificador similar) que no sea utilizado por cualquier otro punto de acceso y enviar este identificador al (a los) punto(s) de acceso solicitante(s).

También se puede dotar al punto de acceso 102 de uno o más identificadores asociados a cada terminal de acceso (por ejemplo, el terminal de acceso 106) al que se permita acceder al punto de acceso 102. Como se describe en más detalle a continuación, esto puede implicar, por ejemplo, almacenar identificadores de terminales de acceso en una base de datos gestionada por una red y/o almacenar identificadores de terminales de acceso en una lista de acceso local en el punto de acceso 102.

En algunas implementaciones, la lista de control de acceso para un punto dado de acceso restringido puede ser administrada en ese punto de acceso restringido. Por ejemplo, como se expone a continuación conjuntamente con la FIG. 13, un usuario puede configurar su punto de acceso mediante un terminal de acceso (por ejemplo, un teléfono celular) o utilizando una página de la Red protegida por contraseña, alojada en el punto de acceso restringido.

Como alternativa, en algunas implementaciones, una lista de control de acceso para cada punto de acceso restringido en una red se gestiona en la red (por ejemplo, la red central). Por ejemplo, como se expone a continuación conjuntamente con la FIG. 4, una lista de control de acceso puede ser gestionada en una página de la red alojada por el operador de red. La gestión de la lista de control de acceso en la red puede proporcionar una o más ventajas en algunos contextos. En algunos aspectos, este enfoque puede permitir una mayor flexibilidad en los criterios. Por ejemplo, el operador puede limitar el acceso a los puntos de acceso restringido si se desea y el operario puede comprobar los registros (por ejemplo, para los terminales de acceso) en el mismo plan de facturación. Además, la red puede ser más fiable que los puntos de acceso individuales. Por lo tanto, la fiabilidad de la lista de control de acceso puede mejorarse. También, ya que la lista de control de acceso tal vez no se envíe al punto de acceso restringido, tal vez no haya necesidad de proporcionar una interfaz directa a los puntos de acceso restringido (por ejemplo, software de aplicación, puertos USB, etc.). Por otra parte, mediante el uso de listas de control de acceso centralizado, puede ser más fácil gestionar múltiples puntos de acceso restringido que pertenecen a una empresa común.

Una vez que se dota a un punto de acceso restringido, se puede anunciar su identificador asignado por el aire. Por ejemplo, el punto de acceso 102 puede difundir su identificador como parte de sus parámetros de sector, o de alguna otra manera adecuada.

Según lo representado por el bloque 206, una vez que se dota a un terminal de acceso, el terminal de acceso puede monitorizar en busca de señales (por ejemplo, señales piloto / baliza) difundidas por puntos de acceso cercanos. Como se expone en detalle más adelante, si el terminal de acceso 106 identifica señales desde el punto de acceso 102 (por ejemplo, en un escenario en el que se permite que el terminal de acceso 106 acceda al punto de acceso 102), el terminal de acceso 106 puede solicitar acceso a ese punto de acceso 102. La identificación de un punto de acceso accesible por el terminal de acceso 106 puede implicar, por ejemplo, la comparación de un identificador asociado al punto de acceso 102 con una lista de confianza 338 de puntos de acceso autorizados (por ejemplo, la lista blanca), mantenida por el terminal de acceso 106. En el ejemplo de la FIG. 3, estas y otras operaciones

relacionadas con el acceso se pueden realizar, por ejemplo, mediante el funcionamiento del controlador de acceso 336.

Tal como se representa mediante el bloque 208, el punto de acceso 102 y/o uno o más nodos de la red (por ejemplo, el nodo de red 110) pueden determinar si se permite o no al terminal de acceso 106 acceder al punto de acceso 102. Esta operación de control de acceso puede implicar, por ejemplo, la confirmación de la identidad del terminal de acceso 106 y la comparación de un identificador del terminal de acceso 106 con una lista de terminales de acceso autorizados, mantenida por el punto de acceso 102 (por ejemplo, una lista de acceso local 340) y / o mantenida por el nodo de red 110 (por ejemplo, una lista de acceso de base de datos de la red 342). En el ejemplo de la FIG. 3, estas y otras operaciones relacionadas con el acceso se pueden realizar, por ejemplo, mediante el funcionamiento del controlador de acceso 336.

Con el panorama anterior en mente, se describirán los detalles adicionales relacionados con la dotación y el control de acceso, con referencia a las FIGs. 4 a 13. Se debería apreciar, en base a las enseñanzas en este documento, que una o más de las operaciones descritas conjuntamente con una figura dada de estas figuras pueden utilizarse conjuntamente con las operaciones descritas en otra de estas figuras. Por conveniencia, estas operaciones se describirán con referencia a los componentes de la FIG. 1. Se debería apreciar que estas operaciones también pueden ser aplicables a otros nodos en una red.

Haciendo referencia inicialmente a la FIG. 4, se tratan varias operaciones relacionadas con la dotación de un punto de acceso restringido.

Tal como se representa mediante el bloque 402, el nodo de red 110 asigna un identificador (por ejemplo, un identificador único) para el punto de acceso restringido. En algunos casos, se garantiza que este identificador sea único dentro de un dominio de operador (por ejemplo, la red completa proporcionada por un operador celular). Por ejemplo, una entidad de red puede mantener una base de datos de identificadores que se utiliza para garantizar la unicidad de cualquier identificador asignado.

El identificador puede adoptar varias formas. En algunas implementaciones, este identificador comprende un identificador de red (por ejemplo, un femto-identificador de red, "FNID"). En algunas implementaciones, el identificador puede comprender un identificador de grupo cerrado de abonados ("ID de CSG"). Como se ha mencionado anteriormente, un conjunto de puntos de acceso restringido (por ejemplo, asociados al mismo dominio administrativo) puede compartir un identificador común (por ejemplo, un ID de CSG). En algunas implementaciones, un conjunto de los FNID puede estar asociado a un CSG común. Por ejemplo, un CSG puede asignarse a una empresa y diferentes FNID pueden asignarse a diferentes puntos de acceso por toda la empresa (por ejemplo, en diferentes edificios). En algunas implementaciones, también se pueden utilizar identificadores adicionales que pueden ser legibles por el usuario (por ejemplo, basados en texto).

El identificador único puede ser dotado de varias maneras. Por ejemplo, en algunos casos, un identificador es escogido y configurado cuando un usuario activa un punto de acceso restringido. Aquí, el identificador puede ser configurado por un operador, en el punto de compra, o de alguna otra manera.

Tal como se representa mediante el bloque 404, se genera una lista de terminales de acceso que están autorizados a acceder al punto de acceso 102 (y, si procede, a cualquier otro punto de acceso en un conjunto definido de puntos de acceso). Esta lista de acceso puede incluir, por ejemplo, los identificadores de terminales de acceso, según se expone en este documento. Por lo tanto, un identificador de este tipo puede identificar un terminal de acceso individual (por ejemplo, un NAI o IMSI o MS ISDN) o un conjunto de uno o más terminales de acceso (por ejemplo, uno o más terminales de acceso asociados a un determinado CSG). Además, la lista de acceso puede especificar permisos (por ejemplo, condiciones de acceso) asociados a un terminal de acceso dado.

En algunas implementaciones, la lista de acceso puede gestionarse mediante el uso de una sede de la Red 344 (por ejemplo, accesible por un ordenador, un teléfono o algún otro dispositivo adecuado). De esta manera, el propietario o usuario del punto de acceso 102 puede acceder a la sede de la Red para añadir, eliminar o editar entradas de terminales de acceso en la lista de acceso. Por ejemplo, para permitir que un terminal de acceso, local o invitado, (por ejemplo, el terminal de acceso 108) acceda al punto de acceso 102, un usuario puede añadir un NAI permanente del terminal de acceso a la lista de acceso mediante una página de la Red. Aquí, varias convenciones de denominación (por ejemplo, identificadores legibles por el usuario, tales como "teléfono de Joe" y similares) pueden estar asociadas a un identificador único de terminal de acceso (por ejemplo, NAI o MS ISDN) y uno o más de estos identificadores pueden ser exhibidos en la página de la Red después de que se añadan a la página de la Red.

Tal como se representa mediante el bloque 406, en algunas implementaciones, la lista de acceso es alojada por el operador de red. Por ejemplo, un operador puede mantener un servidor para la sede en la Red de la lista de acceso. De esta manera, el operador puede aprobar cualquier modificación de la lista de acceso (por ejemplo, denegar entradas para los terminales de acceso de otros operadores).

Tal como se representa mediante el bloque 408, la información de la lista de acceso puede ser enviada luego a cada punto de acceso o a otros nodos de red que realizan el control de acceso asociado a una lista de acceso dada. Por ejemplo, el servidor puede "enviar unilateralmente" la información de la lista de acceso al punto de acceso 102 o el punto de acceso 102 puede "extraer unilateralmente" la información de la lista de acceso del servidor. Como un ejemplo de un modelo de "envío no solicitado", la lista de acceso puede ser enviada desde la sede en la Red del operador a un servidor de configuración que a continuación envía la lista de acceso al punto de acceso 102. Como otro ejemplo, la lista de acceso puede ser enviada desde la sede en la Red del operador, por Internet, al software de aplicación en el punto de acceso 102. Como un ejemplo de un modelo de "extracción unilateral", el punto de acceso 102 puede consultar al servidor de configuración para recibir la versión más reciente de la lista de acceso. Una consulta de este tipo puede tener lugar, por ejemplo, cada vez que el punto de acceso 102 se conecta a la red del operador (por ejemplo, establece una nueva conexión IPSec). Así, en el caso de que el punto de acceso 102 quede "fuera de línea" por un período de tiempo, puede garantizarse que el punto de acceso 102 reciba la versión más reciente de la lista de acceso cada vez que se vuelva a conectar a la red.

Al mantener la lista de acceso en una ubicación distinta al punto de acceso 102, el punto de acceso 102 se libera de la carga de mantener la lista de acceso. Este enfoque puede proporcionar una mejor gestión de la lista de acceso, ya que la lista de acceso puede actualizarse incluso cuando el punto de acceso 102 está fuera de línea. Además, un enfoque de ese tipo puede simplificar la gestión de una lista de acceso que esté asociada a más de un punto de acceso. Por ejemplo, puede definirse una única lista de acceso para un conjunto de puntos de acceso (por ejemplo, asociados a un determinado CSG). En este caso, los puntos de acceso pueden adquirir la lista de acceso desde un único origen, en lugar de tener que coordinarse entre sí para administrar (por ejemplo, actualizar) la lista de acceso entre todos los puntos de acceso.

El uso de una lista de acceso centralizado también puede facilitar el uso de identificadores temporales. Por ejemplo, el punto de acceso 102 puede utilizar un identificador dado durante el tiempo en que se establezca un túnel de IPSec dado. Cuando se establece un nuevo túnel IPSec, la lista de acceso puede configurarse con un conjunto diferente de identificadores. En este caso, el nuevo conjunto de identificadores puede o no identificar los mismos terminales de acceso que la versión anterior de la lista de acceso.

Tal como se representa mediante el bloque 410, el punto de acceso 102 difunde su identificador (por ejemplo, FNID o ID de CSG) por el aire. De esta manera, cualquier terminal de acceso que entre en el área de cobertura del punto de acceso 102 puede identificar el punto de acceso 102 y determinar si se le permite o no acceder al punto de acceso 102.

Haciendo referencia ahora a las FIG. 5 y 6, se describen varias operaciones que pueden utilizarse para dotar a un terminal de acceso. En particular, estas cifras describen técnicas para la dotación a un terminal de acceso de la identidad de uno o más puntos de acceso restringido, a los cuales puede acceder el terminal de acceso.

La FIG. 5 ilustra varias operaciones que pueden realizarse para "enviar unilateralmente" información de lista de acceso a un terminal de acceso (es decir, un modelo de envío no solicitado). En este ejemplo, se supone que un identificador único ha sido asignado al terminal de acceso (por ejemplo, como se ha expuesto anteriormente).

Tal como se representa mediante el bloque 502, en algún momento en el tiempo un terminal de acceso puede ser designado como autorizado para el acceso a uno o más puntos de acceso. Por ejemplo, el propietario de uno o más puntos de acceso puede añadir un terminal de acceso de invitados a la lista de acceso asociada al (a los) punto(s) de acceso, tal como se ha expuesto anteriormente conjuntamente con la FIG. 4.

Tal como se ha representado por el bloque 504, el operador envía un mensaje al terminal de acceso que indica que el terminal de acceso ahora está autorizado a acceder a un punto de acceso o a un conjunto de puntos de acceso. Este mensaje puede incluir un identificador asociado al (a los) punto(s) de acceso (por ejemplo, un FNID o un ID de CSG), así como cualquier limitación que pueda ser aplicable (por ejemplo, límites de tiempo para el acceso de invitados). Tal mensaje puede ser enviado, por ejemplo, cuando se añade un identificador del terminal de acceso 108 a una lista de acceso asociada al punto de acceso 102. Tal mensaje puede también ser enviado de varias maneras. Por ejemplo, la red puede enviar un mensaje del SMS, un mensaje del protocolo de la aplicación (por ejemplo, gestión de dispositivos de la Alianza Móvil Abierta), un mensaje de enlace de radio, una página o algún otro tipo de mensaje, al terminal de acceso para transmitir la información del punto de acceso (por ejemplo, una consulta que pregunta al terminal de acceso 108 si desea o no acceder al punto de acceso 102).

Tal como se representa mediante el bloque 506, el terminal de acceso 108 puede entonces informar al usuario del terminal de acceso 108 que es elegible para acceder al (a los) punto(s) de acceso. Por ejemplo, el terminal de acceso 108 puede mostrar una indicación de la identidad del (de los) punto(s) de acceso, o proporcionar alguna otra forma de indicación. Tal indicación puede comprender, por ejemplo, el identificador asignado al (a los) punto(s) de acceso, o un nombre alternativo (por ejemplo, identificadores legibles por el usuario tales como "la casa de Sue" o similares) que se haya asociado al identificador.

Tal como se representa mediante el bloque 508, el usuario puede a continuación determinar si se habilita o no (por ejemplo, usando un dispositivo de entrada en el terminal de acceso 108) el acceso solicitado al (a los) punto(s) de acceso. En base a la decisión del usuario, el terminal de acceso 108 puede actualizar una lista (por ejemplo, una lista blanca) que mantiene de los puntos de acceso a los cuales está autorizado (por ejemplo, habilitado) a acceder. Como se expone más adelante, el terminal de acceso 108 puede utilizar esta lista para determinar a qué puntos de acceso puede acceder según el terminal de acceso 108 se desplaza por la red. En este caso, el usuario tal vez no tenga que proporcionar ninguna autorización de acceso adicional en el caso de que el terminal de acceso entre en el área de cobertura de un punto de acceso en la lista, ya que el terminal de acceso puede automáticamente "recordar" este punto de acceso. En algunas implementaciones, la lista blanca puede ser actualizada solo después de que se reciba la aprobación del operador de red.

En algunas implementaciones, el terminal de acceso 108 puede enviar al operador un mensaje indicativo de la decisión del usuario. De esta manera, el operador puede optar por modificar la lista de acceso para el (los) punto(s) de acceso, si así lo desea.

Al permitir a un usuario de un terminal de acceso aceptar o rechazar el acceso a un punto de acceso, se puede impedir que un usuario de un punto de acceso habilite unilateralmente un terminal de acceso (por ejemplo, un terminal de acceso de un vecino) para acceder a ese punto de acceso. Así, el usuario de un terminal de acceso puede estar seguro de que su información no se envía a un punto de acceso no autorizado.

Además, este modelo de "envío no solicitado" no requiere que el terminal de acceso esté en la proximidad de un punto de acceso para añadir un punto de acceso a su lista blanca. Además, ya que el terminal de acceso puede recibir el mensaje de "envío no solicitado" solamente cuando ha sido añadido a una lista de acceso, puede reducirse la posibilidad de que un usuario seleccione el punto de acceso incorrecto (por ejemplo, uno al cual no se permita el acceso al terminal de acceso).

La FIG. 6 ilustra varias operaciones que pueden realizarse para "extraer unilateralmente" información de listas de acceso para un terminal de acceso (es decir, un modelo de extracción no solicitada). Una vez más, se supone que un identificador único ha sido asignado al terminal de acceso.

Tal como se representa mediante el bloque 602, en algún momento en el tiempo, un usuario de un terminal de acceso (por ejemplo, el terminal de acceso 108) inicia una búsqueda de puntos de acceso cercanos. Para este fin, el terminal de acceso 108 puede incluir un dispositivo de entrada que el usuario puede controlar (por ejemplo, una opción de menú) para hacer que el receptor 318 monitorice uno o más canales en busca de señales piloto u otras señales desde un punto de acceso.

Tal como se representa mediante el bloque 604, el terminal de acceso 108 informa al usuario de cualquier punto de acceso que fuera detectado como resultado de la búsqueda. Por ejemplo, el terminal de acceso 108 puede mostrar una indicación de la identidad del (de los) punto(s) de acceso detectado(s), o proporcionar alguna otra forma de indicación. De nuevo, tal indicación puede comprender un identificador asignado al (a los) punto(s) de acceso, un nombre alternativo, o alguna otra información adecuada.

Tal como se representa mediante el bloque 606, el usuario puede elegir habilitar el acceso a uno o más puntos de acceso detectados. Por ejemplo, el usuario puede controlar un dispositivo de entrada en el terminal de acceso 108 para seleccionar uno o más puntos de acceso que sean exhibidos por el terminal de acceso 108.

El terminal de acceso, a continuación, intenta acceder al punto de acceso seleccionado, si se desea. Como se expone más adelante, en el caso de que el usuario haya seleccionado el punto de acceso incorrecto (por ejemplo, uno al que el terminal de acceso no está autorizado para acceder), el punto de acceso puede denegar el acceso. El punto de acceso puede a continuación retransmitir esta información al terminal de acceso (por ejemplo, para evitar que esto vuelva a ocurrir en el futuro).

Tal como se representa mediante el bloque 608, en algunas implementaciones, el terminal de acceso 108 puede actualizar una lista que mantiene de los puntos de acceso a los que se le permite acceder (por ejemplo, una lista blanca), en base a la decisión del usuario. De esta manera, el terminal de acceso 108 puede "recordar" un punto de acceso seleccionado de tal manera que no sea necesaria una entrada del usuario para futuras visitas a este punto de acceso (por ejemplo, el terminal de acceso 108 puede conectarse al punto de acceso sin la necesidad de que el usuario inicie otra búsqueda).

Tal como se representa mediante el bloque 610, en algunas implementaciones, se puede utilizar un modelo de "extracción unilateral" para permitir al terminal de acceso 108 acceder a un punto de acceso de manera condicional (por ejemplo, mediante pago por uso). Por ejemplo, varios puntos de acceso (por ejemplo, que pertenecen a un propietario común, tal como un hotel u otra empresa) pueden anunciar todos el mismo identificador único (por ejemplo, FNID o ID de CSG). Cuando el terminal de acceso está cerca de uno de estos puntos de acceso y el usuario del terminal de acceso 108 inicia una búsqueda, el usuario puede elegir conectarse a uno de estos puntos de acceso (por ejemplo, el punto de acceso 102). Cuando el terminal de acceso 108 intenta conectarse al punto de

acceso 102, el punto de acceso 102 no puede comprobar su lista de control de acceso local para ver si el terminal de acceso 108 está autorizado o no para el acceso pero, en cambio, puede permitir que el terminal de acceso 108 realice una conexión inicial. Esta conexión inicial puede implicar, sin embargo, redirigir al usuario a una página en la Red, mediante la cual el terminal de acceso 108 solamente puede recibir servicio desde el punto de acceso 102 si se cumplen ciertas condiciones (por ejemplo, si se realiza un pago). Mediante el uso de este modelo, cualquier terminal de acceso (a diferencia de ciertos terminales de acceso designados) puede obtener acceso al conjunto asociado de puntos de acceso.

Como se ha mencionado anteriormente, un punto de acceso y/o un nodo de red pueden controlar si se permite o no que un terminal de acceso dado acceda al punto de acceso. En algunas implementaciones, el control de acceso para un punto dado de acceso restringido puede ser administrado en ese punto de acceso restringido. En algunas implementaciones, el control de acceso para un punto dado de acceso restringido puede ser administrado en ese punto de acceso restringido con la ayuda de un administrador de control de acceso centralizado (por ejemplo, implementado en un nodo de red). Las FIG. 7 a 11 ilustran varias técnicas que se pueden utilizar para controlar dicho acceso.

Haciendo referencia inicialmente a la FIG. 7, se describen varias operaciones en relación con un escenario en el que un punto de acceso controla el acceso al mismo. En algunos aspectos, el acceso concedido por el punto de acceso puede ser condicional. Por ejemplo, si el punto de acceso determina que el acceso no debería concederse a un determinado servicio, el acceso solicitado puede denegarse unilateralmente. Sin embargo, si el punto de acceso determina que el acceso se debería conceder a un servicio determinado, el punto de acceso puede enviar una solicitud a la red para confirmar si debería o no permitir el acceso.

En algunas implementaciones, un punto de acceso puede controlar (por ejemplo, controlar unilateralmente) el acceso a un servicio local. Por ejemplo, un terminal de acceso puede intentar obtener acceso a un servicio proporcionado en una red local asociada al punto de acceso. Tales servicios pueden incluir, por ejemplo, el acceso a un servidor local (por ejemplo, acceder a audio, vídeo, datos u otro contenido), el acceso a una impresora, etc.

Tal como se representa mediante el bloque 702 de la FIG. 7, en algún momento en el tiempo, un terminal de acceso (por ejemplo, el terminal de acceso 108) comienza el establecimiento de la comunicación con un punto de acceso restringido (por ejemplo, el punto de acceso 102). Conjuntamente con esta operación, el terminal de acceso 108 puede intentar abrir una sesión (o ruta) hasta el punto de acceso 102. Además, la información de sesión asociada puede ser almacenada en la red (por ejemplo, en el nodo de red 110). Para facilitar que el punto de acceso 102 confirme la identidad del terminal de acceso 108, en algunos casos, un identificador del terminal de acceso 108 puede ser parte de la información de la sesión (por ejemplo, ser incluido en la información de contexto del punto de acceso). Este identificador puede comprender, por ejemplo, un identificador permanente (por ejemplo, un NAI), tal como se expone en el presente documento.

Tal como se representa mediante el bloque 704, el punto de acceso 102 puede obtener información para confirmar la identidad del terminal de acceso 108. Por ejemplo, en algunos casos, el punto de acceso 102 puede recibir un identificador (por ejemplo, un identificador temporal) u otra información adecuada directamente desde el terminal de acceso 108 (por ejemplo, por el aire). En algunos casos, el punto de acceso 102 puede recuperar la información de la sesión mencionada anteriormente, que incluye el identificador del terminal de acceso (por ejemplo, un identificador temporal o permanente), de la red (por ejemplo, desde el SRNC). Ventajosamente, en este último escenario, la transmisión del identificador (por ejemplo, el NAI permanente) por el aire puede evitarse.

En los casos en los que se utiliza un identificador temporal (por ejemplo, un NAI temporal), el punto de acceso 102 puede cooperar con la red para asegurar la validez del identificador. Por ejemplo, en algunas implementaciones, el punto de acceso 102 envía el identificador temporal a una entidad de AAA que autentifica el identificador. En algunas implementaciones, el punto de acceso 102 envía el identificador temporal a la red y recibe el identificador permanente asociado en respuesta. En este caso, el punto de acceso 102 puede utilizar el identificador permanente para autentificar el terminal de acceso 108.

Tal como se representa mediante el bloque 706, el punto de acceso 102 compara la información del terminal de acceso (por ejemplo, un identificador temporal o permanente) con la información en su lista de acceso local (por ejemplo, representada por la lista de acceso local 340 en la FIG. 3). Tal como se ha expuesto anteriormente, la lista de acceso local puede estar configurada para incluir un identificador único asociado al terminal de acceso 108 (por ejemplo, NAI, ID de CSG, etc.).

Tal como se representa mediante el bloque 708, el punto de acceso 102, a continuación, puede permitir o rechazar el acceso solicitado en base a la comparación en el bloque 706. Aquí, el punto de acceso 102 puede enviar un mensaje de rechazo al terminal de acceso 108 y/o el punto de acceso 102 puede redirigir el terminal de acceso 108 a un punto de acceso diferente (por ejemplo, mediante el envío de un mensaje de redirección que identifica el punto de acceso macro local).

Tal como se describe a continuación, en algunas implementaciones, el terminal de acceso 102 puede cooperar con la red para autentificar el terminal de acceso 108. Por ejemplo, en el caso de que el identificador de terminal de acceso no esté en la lista de acceso local, el punto de acceso 102 puede enviar una solicitud a un nodo de red, tal como una entidad de AAA, que proporciona autentificación, etc., para los puntos de acceso restringido (por ejemplo, una femto-entidad de AAA implementada, por ejemplo, como una entidad independiente, o mediante la incorporación de la funcionalidad correspondiente en una entidad tradicional de AAA de red). Aquí, el nodo de red puede mantener una lista de control de acceso para el punto de acceso 102 que el nodo de red utiliza para autentificar el terminal de acceso 108 (por ejemplo, de una manera similar como se ha expuesto anteriormente). Además, si procede, el nodo de red puede cooperar con otro nodo de red (por ejemplo, una entidad de AAA para el terminal de acceso 108) para obtener un identificador permanente asociado al terminal de acceso 108, a partir del identificador que fue enviado al punto de acceso 102 por el terminal de acceso 108. El punto de acceso 102 puede entonces permitir o rechazar el acceso solicitado basándose en una respuesta que reciba desde el nodo de red, indicativa de si el terminal de acceso 108 está autorizado o no a acceder al punto de acceso 102. Según las enseñanzas en el presente documento, las funciones de control de acceso se pueden realizar en el punto de acceso u otra entidad de red, tal como una pasarela, un centro de conmutación móvil ("MSC"), un nodo de soporte del GPRS servidor ("SGSN"), un nodo de servicio de datos en paquetes ("PDSN") o una MME, en diversas implementaciones

Haciendo referencia ahora a la FIG. 8, se describen varias operaciones referidas a un escenario en el que la red envía una lista de identificadores de terminales de acceso (por ejemplo, la lista de acceso del punto de acceso) a un punto de acceso, para que el punto de acceso pueda determinar si concede o no una solicitud de acceso de un terminal de acceso. En este ejemplo, las operaciones de los bloques 802 y 804 pueden ser similares a las operaciones de los bloques 702 y 704, descritas anteriormente. En este escenario, sin embargo, el punto de acceso 102 puede no recuperar la información de sesión en algunos casos.

Tal como se representa mediante el bloque 806, el punto de acceso 102 envía una solicitud a la red (por ejemplo, a un nodo de red 110) para autentificar el terminal de acceso 108. En el caso de que el punto de acceso 102 haya obtenido la información de la sesión (por ejemplo, incluyendo información de identificador de terminal de acceso, tal como un MS ISDN, un ID de CSG o un NAI), el punto de acceso 102 puede enviar esta información al nodo de red 110 conjuntamente con la solicitud (por ejemplo, incluida en el mensaje de solicitud). En algunas implementaciones, esta operación puede implicar una solicitud de la lista de identificadores de terminales de acceso. En la práctica, el punto de acceso 102 puede solicitar esta lista en distintos momentos (por ejemplo, cada vez que el punto de acceso se active o se conecte a una red, siempre que un terminal de acceso intente acceder al punto de acceso, de forma periódica, etc.).

Tal como se representa mediante el bloque 808, el nodo de red 110 obtiene un identificador asociado al terminal de acceso 108. Este identificador puede comprender, por ejemplo, una lista de identificadores que indican uno o más grupos de acceso asociados al terminal de acceso. Por ejemplo, el identificador puede comprender una lista de grupos cerrados de abonados, de los cuales es miembro el terminal de acceso 108, una lista de terminales de acceso que tengan permiso para acceder al punto de acceso 102 (por ejemplo, una lista de acceso del punto de acceso 102), o una lista de identificadores de puntos de acceso a los cuales pueda acceder el terminal de acceso 108. La determinación del identificador por el nodo de red 110 puede comprender, por ejemplo, la recepción del identificador desde otro nodo de red (por ejemplo, un HSS) o la obtención del identificador desde una base de datos local. En algunas implementaciones, la determinación del identificador puede implicar la determinación de un identificador permanente, tal como se expone en el presente documento (por ejemplo, en base a un identificador temporal recibido). El nodo de red 110 envía el identificador, o identificadores, obtenido(s) en el bloque 808 al punto de acceso 102 en el bloque 810.

Tal como se representa mediante el bloque 812, el punto de acceso 102 puede a continuación determinar si se permite o se deniega el acceso solicitado en base al (a los) identificador(es) recibido(s). Por ejemplo, el punto de acceso puede comparar el identificador recibido (por ejemplo, un ID de CSG), indicativo de los conjuntos a los cuales pertenece el terminal de acceso 108, con la información (por ejemplo, un ID de CSG) en la lista de acceso local del punto de acceso 102, que es indicativa de los conjuntos a los que pertenece el punto de acceso 102. El punto de acceso 102 puede a continuación permitir o rechazar el acceso solicitado en base a esta comparación.

Haciendo referencia a la FIG. 9, se describen varias operaciones en relación con un escenario en el que una red controla el acceso a un punto de acceso. En este ejemplo, las operaciones de los bloques 902, 904 y 906 pueden ser similares a las operaciones de los bloques 802, 804 y 806, descritas anteriormente. De nuevo, el punto de acceso 102 tal vez no recupere la información de sesión en algunos casos. Además, en algunos casos, el punto de acceso 102 puede enviar su lista de acceso local a la red para su uso en la operación de autentificación.

Tal como se representa mediante el bloque 908, en las implementaciones que utilizan identificadores temporales para identificar uno o más nodos (por ejemplo, terminales de acceso), el nodo de red 110 (por ejemplo, una femto-entidad de AAA) puede determinar un identificador permanente asociado al terminal de acceso 108, en base a un identificador temporal asociado al terminal de acceso 108. Por ejemplo, el punto de acceso 102 puede haber obtenido un identificador temporal desde el terminal de acceso (por ejemplo, en el bloque 902) o desde la

información de la sesión (por ejemplo, en el bloque 904). En tal caso, el punto de acceso 102 puede enviar un identificador temporal (por ejemplo, un NAI temporal) para el terminal de acceso 108, junto con un identificador (por ejemplo, un FNID) del terminal de acceso 102, al nodo de red 110, conjuntamente con la solicitud en el bloque 906. Tal como se ha expuesto anteriormente conjuntamente con la FIG. 7, el nodo de red 110 puede entonces cooperar con otro nodo de red para obtener un identificador permanente del terminal de acceso 108 a partir del identificador temporal.

Tal como se representa mediante el bloque 910, el nodo de red 110 determina si se permite o no que el terminal de acceso 108 acceda al punto de acceso 102. Por ejemplo, el nodo de red 110 puede comparar un identificador del terminal de acceso 108 (por ejemplo, un NAI, un ID de CSG, etc.) con una lista de acceso del punto de acceso 102. En este caso, la lista de acceso puede ser la lista local obtenida a partir del punto de acceso 102 o puede ser una lista de acceso mantenida por la red (por ejemplo, en base a la información obtenida a partir de un servidor de la Red, tal como se ha expuesto anteriormente). El nodo de red 110 puede entonces determinar si se permite o se rechaza el acceso solicitado basándose en esta comparación.

Tal como se representa mediante el bloque 912, el nodo de red 110 envía una indicación de esta determinación al punto de acceso 102. El punto de acceso 102 puede entonces permitir o rechazar el acceso solicitado en base a la indicación recibida (bloque 914). Ventajosamente, en las implementaciones de este tipo, el punto de acceso 102 no necesita estar enterado de la identidad real de los terminales de acceso que acceden al punto de acceso 102. Además, no es necesario enviar la lista de control de acceso para el punto de acceso 102 al punto de acceso 102. En tal implementación, el control de acceso se lleva a cabo enteramente en el nodo de red, de forma transparente para el punto de acceso.

Se pueden usar varias técnicas para administrar los identificadores de terminal de acceso en una red. Tal como se ha mencionado anteriormente, un punto de acceso puede almacenar el identificador válido (por ejemplo, el NAI) utilizado por un terminal de acceso. En algunas implementaciones, este identificador puede seguir siendo válido por un período de tiempo definido. Aquí, si un terminal de acceso vuelve a un punto de acceso dentro del período de tiempo (es decir, el terminal de acceso tiene el mismo identificador durante este tiempo), el punto de acceso puede aceptar el terminal de acceso sin necesidad de obtener la autorización desde la red (por ejemplo, la femto-entidad de AAA). En algunas implementaciones, un operador puede optar por utilizar un identificador temporal o un identificador permanente para los terminales de acceso. Si se utiliza un identificador permanente, los identificadores permanentes se pueden almacenar en los puntos de acceso (por ejemplo, en la lista de acceso local 340) de tal manera que el punto de acceso pueda autentificar de forma independiente los terminales de acceso. Si se utiliza un identificador temporal, el operador puede controlar la frecuencia con la que los puntos de acceso se comprueban ante la red (por ejemplo, la femto-entidad de AAA) para verificar los identificadores almacenados en la lista de acceso local 340.

La FIG. 10 ilustra un ejemplo de las operaciones de control de acceso que se pueden realizar en una aplicación que utiliza la evolución a largo plazo ("LTE") u otra tecnología similar. En este ejemplo, la red (por ejemplo, la red central, en comparación con la red de acceso de radio) controla si se permite o no a un terminal de acceso acceder a un punto de acceso. Además, se describen técnicas para la dotación a terminales de acceso y a puntos de acceso de información de abono a CSG (por ejemplo, información de coincidencia), la imposición del control de acceso (por ejemplo, para la modalidad de reposo o la modalidad activa), la modificación de la dotación de un punto de acceso o terminal de acceso, y la imposición de una lista de CSG, cuando un terminal de acceso lleva a cabo operaciones tales como el encendido, la actualización del área de desplazamiento y el traspaso.

La red (por ejemplo, un servidor de abono doméstico, "HSS", o un servidor de abono a CSG) puede mantener información de abono a CSG para terminales de acceso y puntos de acceso restringido en la red. De una manera similar a la descrita anteriormente, un operador puede proporcionar un servidor de la Red que permite a un usuario gestionar la información de abono a CSG para su(s) punto(s) de acceso restringido. Por ejemplo, un usuario puede modificar su información de abono (por ejemplo, los MS ISDN) usando una sede en la Red. La red puede a continuación aprobar las modificaciones (por ejemplo, entradas de terminales de acceso) realizadas por el usuario y el servidor de la Red puede enviar la información de abono a la red (por ejemplo, un HSS). Aquí, el MS ISDN puede convertirse en un IMSI. La red puede a continuación enviar la información de CSG (por ejemplo, un identificador de CSG único) al (a los) punto(s) de acceso restringido correspondiente(s). Además, la red puede enviar la información de abono a CSG a una MME cuando un terminal de acceso asociado está registrado en la MME.

También, como se ha descrito anteriormente, la dotación de un terminal de acceso (por ejemplo, con una lista de ID de CSG únicos) puede ser aprobada por el propietario del terminal de acceso. Además, el operador también puede aprobar la dotación del terminal de acceso. Aquí, un ID de CSG dado puede estar asociado a un conjunto de uno o más terminales de acceso que están autorizados a recibir por lo menos un servicio de un conjunto de al menos un punto de acceso restringido. En otras palabras, el conjunto de terminales de acceso y el conjunto de puntos de acceso están asociados a un ID de CSG común. También debería apreciarse que un terminal de acceso, o punto de acceso, dado también puede estar asociado a múltiples CSG. En algunos aspectos, la red (por ejemplo, el HSS) puede mantener la información indicativa de la correlación entre un identificador de un terminal de acceso y el ID de

CSG abonado. Además, dado que el HSS está conectado a la MME, la MME puede recuperar la información de CSG y retransmitirla a los puntos de acceso restringido, si lo desea.

Una vez más, la dotación del terminal de acceso puede implicar un "modelo de envío no solicitado" o un modelo de "extracción unilateral". Por ejemplo, en el caso anterior, la red (por ejemplo, un nodo de red) puede enviar un mensaje del SMS al terminal de acceso, para informar al terminal de acceso de un nuevo abono (por ejemplo, identificando uno o más ID de CSG), y el usuario acepta o rechaza el abono. En este último caso, el usuario puede iniciar una búsqueda manual y el terminal de acceso muestra una lista de puntos de acceso cercanos (por ejemplo, ID de CSG legibles por el usuario u otros tipos de identificadores de punto de acceso), de manera que el usuario pueda seleccionar una o más entradas de la lista, si lo desea.

Tal como se representa mediante el bloque 1002 de la FIG. 10, en algún momento el terminal de acceso empieza a acceder al punto de acceso restringido. Por ejemplo, cuando el terminal de acceso 108 determina que está en la vecindad del punto de acceso 102 (por ejemplo, donde el punto de acceso 102 anuncia un ID de CSG que también está asociado al terminal de acceso 108), el terminal de acceso 108 puede enviar una solicitud de registro u otro mensaje adecuado al punto de acceso 102.

Tal como se representa mediante el bloque 1004, el punto de acceso 102 envía una solicitud a la red (por ejemplo, uno o más nodos de la red 110) para autentificar el terminal de acceso 108. En este caso, el (los) nodo(s) de red 110 puede(n) comprender una entidad de gestión de movilidad ("MME") o alguna otra entidad, o entidades, de red adecuada(s). El punto de acceso 102 puede enviar también un identificador (por ejemplo, un ID de CSG asociado al punto de acceso 102) al nodo de red 110, conjuntamente con la solicitud (por ejemplo, incluida en el mensaje de solicitud). Además, la solicitud puede incluir información recibida desde el terminal de acceso 108 (por ejemplo, en el bloque 1002).

Tal como se representa mediante el bloque 1006, el nodo de red 110 obtiene información de contexto asociada al terminal de acceso 108 (por ejemplo, a partir de una MME previa para el terminal de acceso 108, o desde el HSS). Esta información de contexto puede incluir, por ejemplo, un conjunto de identificadores asociados al terminal de acceso 108. Por ejemplo, la información de contexto puede incluir una lista de todas las ID de CSG asociadas al terminal de acceso 108. En algunas implementaciones, el nodo de red 110 puede mantener su propia lista de ID de CSG para cada uno de sus puntos de acceso restringidos. En este caso, el nodo de red 110 puede actualizar su lista cada vez que una entrada se cambie en el servidor de la Red.

Tal como se representa mediante el bloque 1008, el nodo de red 110 determina si se permite o no que el terminal de acceso 108 acceda al punto de acceso 102. Por ejemplo, el nodo de red 110 determina si un identificador del punto de acceso 102 (por ejemplo, indicativo de un CSG al que pertenece el punto de acceso 102) está o no en una lista de identificadores asociados al terminal de acceso 108 (por ejemplo, indicativo de todos los CSG a los que pertenece el terminal de acceso 108).

La determinación del bloque 1008 se puede realizar en diferentes nodos de red. Por ejemplo, en algunas implementaciones, esta determinación puede tomarse en una MME que obtiene y/o mantiene los identificadores asociados al punto de acceso 102 y al terminal de acceso 108.

En algunas implementaciones, esta determinación puede tomarse en otro nodo de red, tal como un HSS. Por ejemplo, la MME puede enviar una solicitud al HSS para determinar si el terminal de acceso 108 está o no autorizado a acceder al punto de acceso 102. Conjuntamente con una solicitud de este tipo, la MME puede enviar información (por ejemplo, identificadores tales como un IMSI y un ID de CSG) al HSS en algunos casos. Además, en algunos casos, el HSS puede obtener y mantener tal información por sí mismo. Después de determinar si se permite o no el acceso, el HSS envía una respuesta correspondiente de nuevo a la MME.

Tal como se representa mediante el bloque 1010, la MME envía una respuesta al punto de acceso 102 en base a la determinación de la MME o en base a la determinación de otro nodo de red (por ejemplo, un HSS). En base a esta respuesta, el punto de acceso 102 puede entonces permitir o denegar el acceso mediante el punto de acceso 108.

La FIG. 11 ilustra operaciones que pueden utilizarse conjuntamente con una operación de traspaso. Por ejemplo, el terminal de acceso 108 inicialmente puede recibir servicio del punto de acceso 104 y, en un momento posterior en el tiempo, el terminal de acceso 108 es traspasado al punto de acceso 102 y a continuación recibe servicio de ese nodo.

Tal como se representa mediante el bloque 1102, la red (por ejemplo, un HSS) puede mantener la información de contexto para cada terminal de acceso en el sistema. Como se ha mencionado anteriormente, esta información de contexto puede incluir una lista (por ejemplo, una lista blanca) indicativa de todos los conjuntos de acceso (por ejemplo, los CSG), a los cuales pertenece el terminal de acceso 108.

Tal como se representa mediante el bloque 1104, la red (por ejemplo, una MME) captura el contexto para el terminal de acceso dado y proporciona el contexto a un punto de acceso restringido cuando ese terminal de acceso se activa

en el punto de acceso restringido. Con referencia al ejemplo de la FIG. 3, cuando el terminal de acceso 108 se activa (por ejemplo, se enciende) en el punto de acceso 104, el nodo de red 110 puede enviar la información de contexto para el terminal de acceso 108 al punto de acceso 104. De esta manera, el terminal de acceso 108 puede inicialmente recibir servicio del punto de acceso 104.

Tal como se representa mediante el bloque 1106, en algún momento en el tiempo, el terminal de acceso 108 puede ser traspasado al punto de acceso 102. Por ejemplo, si el terminal de acceso 108 se aleja del punto de acceso 104, los informes de medición desde el terminal de acceso 108 pueden indicar que la intensidad de señal de las señales recibidas desde el punto de acceso 102 es ahora más alta que la intensidad de señal de las señales recibidas desde el punto de acceso 104. En este caso, la red puede iniciar un traspaso desde el punto de acceso 104 hasta el punto de acceso 102.

Tal como se ha representado mediante los bloques 1106 y 1108, conjuntamente con este traspaso, el punto de acceso 104 (es decir, el punto de acceso de origen) puede recibir un identificador asociado al punto de acceso de destino (es decir, el punto de acceso 102), como, por ejemplo, un ID de CSG. Por ejemplo, esta información puede ser recibida desde el terminal de acceso 108. El punto de acceso 104 puede entonces determinar si el terminal de acceso 108 está o no autorizado para acceder al punto de acceso 102 en base a este identificador. Por ejemplo, el punto de acceso 104 puede comparar el identificador con una lista que especifica los puntos de acceso a los cuales se permite acceder al terminal de acceso 108 (por ejemplo, una lista blanca, tal como una lista de los ID de CSG, a partir de la información de contexto para el terminal de acceso 108).

Tal como se representa mediante el bloque 1110, si el terminal de acceso 108 no está autorizado a acceder al punto de acceso 102 (por ejemplo, el ID de CSG del punto de acceso 102 no está en la lista de los ID de CSG del terminal de acceso 108), no puede llevarse a cabo la operación de traspaso. Por ejemplo, el punto de acceso 102 puede enviar un mensaje al nodo de red 110 para terminar la operación de traspaso. Además, o como alternativa, el punto de acceso 102 puede enviar un mensaje de rechazo y/o redirección al punto de acceso 108 (por ejemplo, como se ha expuesto anteriormente).

Tal como se representa mediante el bloque 1112, la operación de traspaso puede avanzar si el terminal de acceso 108 está autorizado a acceder al punto de acceso 102 (por ejemplo, el ID de CSG del punto de acceso 102 está en la lista de los ID de CSG del terminal de acceso 108). En consecuencia, la red (por ejemplo, la MME) puede enviar la información de contexto para el terminal de acceso 108 al punto de acceso 102 o el punto de acceso 102 puede recibir esta información desde el punto de acceso 104.

Tal como se representa mediante el bloque 1114, el punto de acceso 102 puede determinar si el terminal de acceso 108 está o no autorizado para acceder al punto de acceso 102. Por ejemplo, de forma similar a lo que se ha expuesto anteriormente, el punto de acceso 102 puede comparar su identificador (por ejemplo, un ID de CSG) con una lista que especifica los puntos de acceso a los cuales se permite acceder al terminal de acceso 108 (por ejemplo, una lista de los ID de CSG a partir de la información de contexto para el terminal de acceso 108).

Tal como se representa mediante el bloque 1116, en algunas implementaciones, el punto de acceso 102 puede enviar una solicitud a la red (por ejemplo, la MME) para confirmar si el traspaso se debería realizar o no (por ejemplo, conjuntamente con una solicitud de conmutación de trayecto). Por ejemplo, tal como se ha expuesto anteriormente, el punto de acceso 102 puede enviar una solicitud (por ejemplo, incluyendo optativamente un identificador asociado al terminal de acceso 108 y el ID de CSG para el punto de acceso, si es necesario) al nodo de red 110 para determinar si debe o no permitirse el acceso del terminal de acceso 108 al punto de acceso 102.

En situaciones en las que un terminal de acceso necesite acceder al punto de acceso de destino sin previa preparación del traspaso (por ejemplo, durante un fallo del enlace de radio), un punto de acceso de destino puede capturar el contexto del terminal de acceso desde el punto de acceso de origen. Tal como se ha mencionado anteriormente, este contexto incluye una lista de los CSG del terminal de acceso. Por lo tanto, el punto de acceso de destino puede determinar si se permite o no al terminal de acceso acceder al punto de acceso de destino.

Tal como se representa mediante el bloque 1118, en base a la determinación en el bloque 1114 (y, optativamente, el bloque 1116), el traspaso se permite o se rechaza. Si se permite el traspaso, el punto de acceso 102 entonces se convierte en el punto de acceso de servicio para el terminal de acceso 108. Por el contrario, si no se permite el traspaso, el traspaso puede terminarse (por ejemplo, como se ha expuesto anteriormente junto con el bloque 1110).

Con referencia ahora a la FIG. 12, en algunas implementaciones, se puede utilizar un punto de acceso restringido para dotar a un terminal de acceso. Con fines ilustrativos, los ejemplos siguientes describen ejemplos en los que un terminal de acceso es dotado (por ejemplo, configurado) con una lista de itinerancia preferida ("PRL"). Se debería apreciar, sin embargo, que se puede dotar a un terminal de acceso con otros tipos de información, según las enseñanzas en el presente documento.

Tal como se representa mediante el bloque 1202, los terminales de acceso en una red (por ejemplo, terminales de acceso cualesquiera, que puedan acceder a un punto de acceso restringido) pueden configurarse inicialmente con

una PRL por omisión (por ejemplo, la lista comprende o especifica una configuración por omisión). Por ejemplo, el terminal de acceso 106 puede ser configurado por el operador de la red cuando el terminal de acceso 106 es comprado por un usuario. Tal PRL puede especificar, por ejemplo, un identificador de sistema ("SID") por omisión, un identificador de red ("NID") por omisión y una frecuencia por omisión para la adquisición inicial de cualquier punto de acceso restringido que se pueda desplegar en la red. Aquí, todos los terminales de acceso anteriores pueden configurarse con la PRL por omisión. De esta manera, cada terminal de acceso puede localizar, y acceder a, un punto de acceso restringido para las operaciones de dotación. En algunos aspectos, la información de PRL por omisión (por ejemplo, el SID y/o el NID) puede corresponder a uno o más puntos de acceso asociados a una prioridad máxima. Por ejemplo, el terminal de acceso puede configurarse para buscar (por ejemplo, buscar en primer lugar) un punto de acceso preferido especificado, o puntos de acceso preferidos especificados (por ejemplo, puntos de acceso de origen).

En algunos aspectos, los parámetros de la PRL por omisión pueden reservarse para las operaciones relacionadas con puntos de acceso restringido. Por ejemplo, el SID por omisión puede ser reservado para los puntos de acceso restringido por el operador de red. Mediante el uso de un SID tal, puede evitarse que los terminales de acceso que no estén configurados para acceder a los puntos de acceso restringido (por ejemplo, terminales de acceso configurados solo para su uso en una macro-red) intenten el registro en puntos de acceso restringido. Además, el NID por omisión se puede reservar para los procedimientos de inicialización relacionados con puntos de acceso restringido. Además, la frecuencia por omisión puede definirse como una frecuencia común, para ser utilizada por los puntos de acceso restringido en la red, para la transmisión de balizas para procedimientos de dotación. En algunos casos, la frecuencia por omisión puede ser la misma que la frecuencia de funcionamiento de un punto de macro-acceso, o una frecuencia de funcionamiento de un punto de acceso restringido.

La PRL por defecto también puede incluir información de selección de macro-sistema. Por ejemplo, la PRL por omisión puede incluir identificadores y frecuencias que pueden utilizarse para acceder a los puntos de macro-acceso en la red.

Tal como se representa mediante el bloque 1204, los puntos de acceso restringido en el sistema (por ejemplo, el punto de acceso 102) están configurados para transmitir una baliza de arranque. En algunos aspectos, esta baliza de arranque puede comprender una baliza temporal que se utiliza conjuntamente con la dotación proporcionada por el punto de acceso 102. Aquí, la baliza de arranque puede difundirse según los parámetros genéricos de PRL expuestos anteriormente (por ejemplo, la baliza puede comprender o especificar una configuración por omisión). Por ejemplo, la baliza de arranque (por ejemplo, una baliza por omisión) puede ser transmitida a la frecuencia por omisión, y puede incluir el SID por omisión y el NID por omisión (por ejemplo, enviados en mensajes de sobrecarga).

La baliza de arranque puede ser transmitida en un nivel de potencia muy bajo que es mucho menor que la potencia de transmisión de baliza durante las operaciones normales de punto de acceso (por ejemplo, cuando el punto de acceso está configurado en una modalidad de funcionamiento no de inicialización, tal como una modalidad de funcionamiento normal). Por ejemplo, la potencia de transmisión de la baliza de arranque puede dar como resultado una gama de cobertura (por ejemplo, un radio) para la baliza de arranque, del orden de un metro o menos.

En algunas implementaciones, el punto de acceso 102 puede transmitir balizas de arranque cuando el punto de acceso está en una modalidad de dotación (por ejemplo, configuración o inicialización). En algunas implementaciones, un usuario puede utilizar un dispositivo de entrada para colocar el punto de acceso 102 en la modalidad de configuración cuando el usuario desee dotar inicialmente, o volver a dotar, al terminal de acceso 106. Por ejemplo, se puede dotar un terminal de acceso cuando se instala por primera vez un punto de acceso, cuando se adquiere un terminal de acceso por primera vez o cuando la PRL de un terminal de acceso fue actualizada por una macro-red (por ejemplo, conjuntamente con un cambio en la lista de itinerancia, los viajes internacionales, etc.), lo cual dio como resultado que fuera sobrescrita la PRL dotada por el punto de acceso (como se expone más adelante).

Tal como se representa mediante el bloque 1206, cuando el terminal de acceso 106 dotado de la PRL por defecto se coloca cerca del punto de acceso restringido 102, funcionando en una modalidad de dotación, el terminal de acceso 106 puede recibir la baliza de arranque transmitida por el punto de acceso 102. En respuesta, el terminal de acceso 106 puede enviar un mensaje al punto de acceso 102 para iniciar las operaciones de dotación. En algunas implementaciones, este mensaje puede incluir la PRL actualmente usada por el terminal de acceso 106. En algunas implementaciones, un usuario del terminal de acceso 106 puede iniciar la dotación mediante la selección de una característica correspondiente en el terminal de acceso (por ejemplo, la marcación de un número definido).

Tal como se representa mediante el bloque 1208, el punto de acceso 102 (por ejemplo, el controlador de dotación 328) puede definir una nueva PRL para el terminal de acceso 106 (por ejemplo, para operaciones móviles normales). La nueva PRL puede incluir información del macro-sistema como en la PRL por omisión, pero la información de inicialización de la PRL por omisión puede eliminarse. En su lugar, puede añadirse nueva información de PRL (por ejemplo, la lista comprende o especifica una nueva configuración). En algunos aspectos, la información de PRL nueva puede ser específica para el punto de acceso 102 (por ejemplo, la nueva PRL puede ser diferente a la PRL dotada por otros puntos de acceso). Por ejemplo, una nueva PRL puede especificar el SID que está reservado para

todos los puntos de acceso restringido, como se ha expuesto anteriormente, un NID que es único para el punto de acceso 102 (por ejemplo, un femto-NID, "FNID"), y un parámetro de frecuencia que indica la frecuencia de funcionamiento del punto de acceso 102. Este parámetro de frecuencia puede ser el mismo que, o diferente a, la frecuencia por omisión. En algunos aspectos, la información de PRL nueva (por ejemplo, el SID y/o el NID) puede corresponder a uno o más puntos de acceso asociados a una prioridad más alta. Por ejemplo, el terminal de acceso 106 puede configurarse para buscar (por ejemplo, buscar en primer lugar) un punto de acceso preferido especificado, o puntos de acceso preferidos especificados (por ejemplo, puntos de acceso domésticos).

El punto de acceso 102 puede obtener información de PRL de macro-sistema de varias maneras. En algunas implementaciones, el punto de acceso 102 puede solicitar esta información de PRL desde el punto de macro-acceso (por ejemplo, mediante el nodo de red 110 o por el aire). En algunas implementaciones, el punto de acceso 102 puede recibir esta información de PRL desde un terminal de acceso (por ejemplo, el terminal de acceso 108). Por ejemplo, el punto de acceso 102 puede incluir una función por el aire. En este caso, el punto de acceso 102 puede enviar un mensaje (por ejemplo, una solicitud de configuración de SSPR) para solicitar la PRL actual del terminal de acceso (que puede incluir la macro-información de PRL actual, como se ha expuesto anteriormente), y el terminal de acceso puede responder mediante el envío de su PRL actual por el aire al punto de acceso 102.

Una vez que el punto de acceso 102 define una nueva PRL, el punto de acceso 102 envía (por ejemplo, envía unilateralmente) la PRL al terminal de acceso 106. Por ejemplo, el punto de acceso 102 puede enviar una PRL al terminal de acceso por el aire (por ejemplo, mediante OTASP u OTAPA).

Ventajosamente, al dotar el terminal de acceso 106 mediante el punto de acceso 102, según se ha expuesto anteriormente, el operador de red no necesita mantener información específica del terminal de acceso (por ejemplo, información de PRL). Puede ser deseable, sin embargo, configurar el punto de acceso 102 para que haga actualizaciones periódicas para la PRL del terminal de acceso. Por ejemplo, la PRL puede actualizarse cada noche y enviarse al terminal de acceso 106 por el aire. Además, para evitar que un punto de acceso, de un conjunto de puntos de acceso relacionados, sobrescriba la dotación de información de PRL con otro punto de acceso del conjunto, cada punto de acceso puede configurarse para actualizar simplemente la información de PRL actual del terminal de acceso. Por ejemplo, el punto de acceso 102 puede consultar el terminal de acceso 106 en cuanto a su información de PRL, por lo que el punto de acceso 102 añadirá su propia información de sistema de PRL a la PRL actual del terminal de acceso 106, en lugar de sobrescribir la información de la PRL actual.

Tal como se representa mediante el bloque 1210, una vez que se dota al terminal de acceso 106 con la nueva información de PRL, el terminal de acceso 106 utilizará esta información para identificar los puntos de acceso a los que pueda acceder. Por ejemplo, en el caso de que el terminal de acceso 106 determina que el punto de acceso 102 está en la proximidad (por ejemplo, después de que el punto de acceso se haya configurado para una modalidad de funcionamiento normal), el terminal de acceso 106 puede dar preferencia a ser servido por el punto de acceso 102 en lugar de cualquier otro punto de acceso (por ejemplo, un punto de maco-acceso) que sea detectado por el terminal de acceso 106.

Haciendo referencia ahora a la FIG. 13, se describen diversas técnicas para el control de acceso restringido (por ejemplo, la asociación) en un punto de acceso. En este ejemplo, un punto de acceso puede configurarse con una lista local de terminales de acceso a los que se permite acceder a uno o más servicios proporcionados por el punto de acceso. El punto de acceso puede entonces conceder o denegar el acceso en base a la lista local. Ventajosamente, en algunos aspectos, un esquema de este tipo puede permitir que el propietario de un punto de acceso dé servicio temporal a terminales de acceso invitados (por ejemplo, añadiendo / eliminando estos terminales de acceso a / de la lista) sin la participación de un operador de red.

Tal como se representa mediante el bloque 1302, un punto de acceso restringido (por ejemplo, el punto de acceso 102) está configurado con una lista de acceso (por ejemplo, representada por la lista de acceso local 340 en la FIG. 3). Por ejemplo, el propietario del punto de acceso 102 puede configurar una lista de identificadores (por ejemplo, números de teléfono) de terminales de acceso a los que se permite utilizar uno o más servicios prestados por el punto de acceso 102. En algunas implementaciones, el control sobre qué terminales de acceso pueden acceder al punto de acceso 102 puede, de este modo, recaer en el propietario del punto de acceso 102, en lugar de un operador de red.

El punto de acceso 102 puede recibir dotación de varias maneras. Por ejemplo, el propietario puede utilizar una interfaz de la Red alojada por el punto de acceso 102 para configurar el punto de acceso 102.

Además, los diferentes terminales de acceso pueden recibir diferentes niveles de acceso. Por ejemplo, a los terminales de acceso invitados se les puede dar acceso temporal en base a varios criterios. También, en algunas implementaciones, a un terminal de acceso doméstico se le puede asignar una mejor calidad de servicio que a un terminal de acceso para invitados. Además, algunos terminales de acceso (por ejemplo, terminales de acceso para invitados) pueden tener acceso a ciertos servicios (por ejemplo, servicios locales, tales como un servidor de multimedios o algún otro tipo de servidor de información) sin la participación de la autentificación por parte de un operador de red. También, en algunos casos, la lista de acceso local 340 puede utilizarse como una brecha de

parada inicial en el punto de acceso 102, por lo cual la autentificación real (por ejemplo, para una llamada telefónica) puede ser realizada por la red para evitar que la seguridad de la red se vea comprometida.

Tal como se representa mediante el bloque 1304, el punto de acceso 102 puede enviar la información de identificador de terminal de acceso que fuera configurada en el bloque 1302 (por ejemplo, la lista de acceso local 340) a una base de datos de red (por ejemplo, un centro de autentificación o un registro de ubicación local, "AC / HLR ") y solicitar otra información de identificación asociada a los terminales de acceso correspondientes. Por ejemplo, el punto de acceso 102 puede enviar un número de teléfono del terminal de acceso 106 al nodo de red 110 (por ejemplo, que comprende una base de datos de HLR) y recibir un número de serie electrónico ("ESN") o una identidad de abonado móvil internacional ("IMSI ") que se asigna al terminal de acceso 106 desde el nodo de red 110.

Tal como se representa mediante el bloque 1306, el punto de acceso 102 pueden anunciar su información de identificación (por ejemplo, tal como se expone en el presente documento). Por ejemplo, el punto de acceso 102 puede anunciar la información de SID y FNID, tal como se ha expuesto anteriormente.

Tal como se representa mediante el bloque 1308, un terminal de acceso que está dotado para acceder al punto de acceso 102 puede determinar que se encuentra en la proximidad del punto de acceso 102 al recibir la información de identificación anunciada. Por ejemplo, puede dotarse de una PRL al terminal de acceso 106, mediante el punto de acceso 102, como se ha expuesto anteriormente, o el terminal de acceso 106 puede dotarse de una PRL que incluya el SID del punto de acceso restringido, un NID comodín y una o más frecuencias operativas que son utilizadas por el punto de acceso 102, o bien el terminal de acceso 106 puede ser dotado de alguna otra manera que le permita identificar el punto de acceso 102 (por ejemplo, dotado de una lista de zonas de usuario preferidas). El terminal de acceso 106 puede entonces intentar registrarse en el punto de acceso 102, como resultado de recibir un SID diferente (por ejemplo, que puede representar una zona diferente de la macro-zona para el registro basado en zonas). Así, en algunos casos, el terminal de acceso puede intentar automáticamente acceder al punto de acceso 102. En otros casos, sin embargo, un usuario puede controlar si el terminal de acceso 106 accede o no al punto de acceso 102 (por ejemplo, el usuario proporciona la entrada mediante un dispositivo de entrada en respuesta a una indicación de puntos de acceso detectados, emitida por el terminal de acceso 106). Conjuntamente con este registro, el terminal de acceso 106 puede enviar su identificador (por ejemplo, su ESN, IMSI, etc.) al punto de acceso 102 (por ejemplo, mediante un canal de acceso).

Tal como se representa mediante los bloques 1310 y 1312, el punto de acceso 102 determina si se permite o no que el terminal de acceso 106 acceda al punto de acceso 102. Por ejemplo, el punto de acceso 102 puede determinar si el identificador recibido desde el terminal de acceso 106 está o no enumerado en la lista de acceso local 340. Se debería apreciar que puede utilizarse información de autentificación distinta a los ESN e IMSI en diferentes implementaciones. Por ejemplo, el punto de acceso 102 puede recibir información de números de origen de llamadas mediante mensajes de inactividad, y utilizar esta información para la autentificación (por ejemplo, para compararla con un número de llamador recibido desde el terminal de acceso 106 mediante un mensaje de registro, o de alguna otra manera).

Tal como se representa mediante el bloque 1314, si al terminal de acceso 106 no se le permite el acceso (por ejemplo, el identificador del terminal de acceso recibido no está en la lista de acceso local 340), el punto de acceso 102 puede denegar el acceso. Por ejemplo, el punto de acceso 102 puede enviar un mensaje de rechazo de registro al terminal de acceso 106. Además, o como alternativa, el punto de acceso 102 puede enviar un mensaje de redirección de servicio al terminal de acceso 106. Este mensaje puede incluir, por ejemplo, información (por ejemplo, SID, NID, frecuencia de funcionamiento) que identifica un punto de acceso alternativo (por ejemplo, una macro-red local) al cual puede acceder el terminal de acceso 106.

Tal como se representa mediante el bloque 1316, si al terminal de acceso 106 se le permite el acceso (por ejemplo, el identificador del terminal de acceso recibido está en la lista de acceso local 340), el punto de acceso 102 puede conceder acceso a ciertos servicios. Por ejemplo, como se ha expuesto anteriormente, el punto de acceso 102 puede conceder acceso a los servicios locales ofrecidos por una red local.

Además, o como alternativa, el punto de acceso 102 puede pasar la información de registro al nodo de red 110 (por ejemplo, el HRL de la macro-red) para su autentificación y registro del terminal de acceso 106. El nodo de red 110 puede entonces responder con un mensaje de aceptación o rechazo de registro. En respuesta, el punto de acceso 102 puede enviar un mensaje correspondiente al terminal de acceso 106. Si está autorizado, el punto 106 de acceso obtiene a continuación el servicio de solicitud del punto de acceso 102 (por ejemplo, acceso a la red).

Se debería apreciar que las técnicas anteriores pueden implementarse de diversas maneras según las enseñanzas en este documento. Por ejemplo, se puede utilizar información de autentificación, que sea diferente a la información específicamente mencionada anteriormente (por ejemplo, el ESN, el IMSI, los ID de CSG), en un aparato o procedimiento practicado en base a las enseñanzas en este documento.

En algunos aspectos, las enseñanzas en el presente documento pueden utilizarse en una red que incluya cobertura de macro-escala (por ejemplo, una red celular de área amplia, tal como una red 3G, normalmente denominada red

macro-celular, o una WAN) y cobertura a menor escala (por ejemplo, un entorno de red basado en un domicilio o en un edificio, normalmente denominado LAN). A medida que un terminal de acceso se desplaza a través de una red de este tipo, el terminal de acceso puede recibir servicio en determinadas ubicaciones por medio de puntos de acceso que proporcionan macro-cobertura, mientras que el terminal de acceso puede recibir servicio en otras ubicaciones por medio de puntos de acceso que proporcionan cobertura a menor escala. En algunos aspectos, los nodos de menor cobertura pueden usarse para proporcionar crecimiento de capacidad incremental, cobertura dentro de un edificio y diferentes servicios (por ejemplo, para una experiencia de usuario más robusta). En la descripción proporcionada en el presente documento, un nodo que proporciona cobertura en un área relativamente grande puede denominarse un macro-nodo. Un nodo que proporciona cobertura en un área relativamente pequeña (por ejemplo, un domicilio) puede denominarse un femto-nodo. Un nodo que proporciona cobertura en un área que es más pequeña que una macro-área y mayor que una femto-área puede denominarse un pico-nodo (por ejemplo, proporcionando cobertura dentro de un centro comercial).

Una célula asociada a un macro-nodo, un femto-nodo o un pico-nodo puede denominarse macro-célula, femto-célula o pico-célula, respectivamente. En algunas implementaciones, cada nodo puede estar asociado a (por ejemplo, estar dividido en) una o más células o sectores.

En diversas aplicaciones puede usarse otra terminología para hacer referencia a un macro-nodo, un femto-nodo o un pico-nodo. Por ejemplo, un macro-nodo puede estar configurado, o mencionado, como un nodo de acceso, una estación base, un punto de acceso, un eNodoB, una macro-célula, etc. Asimismo, un femto-nodo puede estar configurado o mencionado como un NodoB doméstico, un eNodoB doméstico, una estación base de punto de acceso, una femto-célula, etc.

La FIG. 14 ilustra un sistema de comunicación inalámbrica 1400, configurado para dar soporte a un determinado número de usuarios, en el que pueden implementarse las enseñanzas en el presente documento. El sistema 1400 proporciona comunicación para múltiples células 1402, tales como, por ejemplo, las macro-células 1402A a 1402G, donde cada célula recibe servicio de un correspondiente nodo de acceso 1404 (por ejemplo, los puntos de acceso 1404A a 1404G). Tal como se muestra en la FIG. 14, los terminales de acceso 1406 (por ejemplo, los terminales de acceso 1406A a 1406L) pueden estar dispersos en varias ubicaciones por todo el sistema a lo largo del tiempo. Cada terminal de acceso 1406 puede comunicarse con uno o más puntos de acceso 1404 en un enlace directo (“FL”) y/o un enlace inverso (“RL”) en un momento dado, en función de si el terminal de acceso 1406 está activo o no, y de si está o no en un traspaso suave, por ejemplo. El sistema de comunicación inalámbrica 1400 puede prestar servicio en una gran región geográfica. Por ejemplo, las macro-células 1402A a 1402G pueden abarcar unos pocos bloques de un vecindario o varios kilómetros en un entorno rural.

La FIG. 15 ilustra un sistema de comunicación 1500 ejemplar, en el que uno o más femto-nodos están desplegados dentro de un entorno de red. Específicamente, el sistema 1500 incluye múltiples femto-nodos 1510 (por ejemplo, los femto-nodos 1510A y 1510B) instalados en un entorno de red a escala relativamente pequeña (por ejemplo, en uno o más domicilios de usuario 1530). Cada femto-nodo 1510 puede estar acoplado a una red de área amplia 1540 (por ejemplo, Internet) y a una red central de operador móvil 1550, mediante un encaminador de DSL, un módem por cable, un enlace inalámbrico u otros medios de conectividad (no mostrados). Como se expondrá posteriormente, cada femto-nodo 1510 puede estar configurado para dar servicio a terminales de acceso 1520 asociados (por ejemplo, el terminal de acceso 1520A) y, optativamente, a terminales de acceso 1520 foráneos (por ejemplo, el terminal de acceso 1520B). Dicho de otro modo, el acceso a los femto-nodos 1510 puede restringirse de modo que un terminal de acceso dado 1520 pueda recibir servicio desde un conjunto de femto-nodos designados 1510 (por ejemplo, domésticos), pero no pueda recibir servicio desde cualquier femto-nodo no designado 1510 (por ejemplo, un femto-nodo de un vecino 1510).

La FIG. 16 ilustra un ejemplo de un mapa de cobertura 1600 en el que están definidas varias áreas de rastreo 1602 (o áreas de encaminamiento o áreas de ubicación), cada una de las cuales incluye varias macro-áreas de cobertura 1604. Aquí, las áreas de cobertura asociadas a las áreas de rastreo 1602A, 1602B y 1602C están delimitadas mediante líneas gruesas y las macro-áreas de cobertura 1604 están representadas mediante hexágonos. Las áreas de rastreo 1602 incluyen además femto-áreas de cobertura 1606. En este ejemplo, cada una de las femto-áreas de cobertura 1606 (por ejemplo, la femto-área de cobertura 1606C) se muestra dentro de una macro-área de cobertura 1604 (por ejemplo, la macro-área de cobertura 1604B). Sin embargo, debería apreciarse que una femto-área de cobertura 1606 puede no quedar completamente dentro de una macro-área de cobertura 1604. En la práctica, un gran número de femto-áreas de cobertura 1606 pueden estar definidas con un área de rastreo 1602 o una macro-área de cobertura 1604 dadas. Además, una o más pico-áreas de cobertura (no mostradas) pueden definirse dentro de un área de rastreo 1602 o de una macro-área de cobertura 1604 dadas.

Haciendo de nuevo referencia a la FIG.15, el propietario de un femto-nodo 1510 puede abonarse a un servicio móvil tal como, por ejemplo, un servicio móvil de 3G, ofrecido a través de la red central de operador móvil 1550. Además, un terminal de acceso 1520 puede ser capaz de funcionar tanto en macro-entornos como en entornos de red de menor escala (por ejemplo, residenciales). Dicho de otro modo, en función de la ubicación actual del terminal de acceso 1520, el terminal de acceso 1520 podrá recibir servicio por medio de un punto de acceso de macro-célula 1560, asociado a la red central de operador móvil 1550, o por medio de uno cualquiera entre un conjunto de femto-

nodos 1510 (por ejemplo, los femto-nodos 1510A y 1510B que residen dentro de un domicilio de usuario 1530 correspondiente). Por ejemplo, cuando un abonado no está en casa, recibe servicio desde un punto de macro-acceso estándar (por ejemplo, el punto de acceso 1560) y, cuando el abonado está en casa, recibe servicio desde un femto-nodo (por ejemplo, el nodo 1510A). En este caso, debería apreciarse que un femto-nodo 1510 puede ser retro-compatible con terminales de acceso existentes 1520.

Un femto-nodo 1510 puede desplegarse en una única frecuencia o, como alternativa, en múltiples frecuencias. Según la configuración particular, la única frecuencia, o una o más de las múltiples frecuencias, pueden solaparse con una o más frecuencias usadas por un punto de macro-acceso (por ejemplo, un punto de acceso 1560).

En algunos aspectos, un terminal de acceso 1520 puede estar configurado para conectarse a un femto-nodo preferido (por ejemplo, el femto-nodo doméstico del terminal de acceso 1520) toda vez que tal conectividad sea posible. Por ejemplo, toda vez que el terminal de acceso 1520 esté dentro del domicilio del usuario 1530, puede desearse que el terminal de acceso 1520 se comunique únicamente con el femto-nodo doméstico 1510.

En algunos aspectos, si el terminal de acceso 1520 funciona dentro de la red macro-celular 1550, pero no reside en su red más preferida (por ejemplo, según lo definido en una lista de itinerancia preferida), el terminal de acceso 1520 puede seguir buscando la red más preferida (por ejemplo, el femto-nodo preferido 1510) usando una Re-selección de Mejor Sistema (“BSR”), que puede implicar un recorrido periódico de sistemas disponibles, para determinar si hay o no mejores sistemas actualmente disponibles, y acciones posteriores para la asociación con tales sistemas preferidos. Con la entrada de adquisición, el terminal de acceso 1520 puede limitar la búsqueda para banda y canal específicos. Por ejemplo, la búsqueda del sistema más preferido puede repetirse periódicamente. Tras descubrir un femto-nodo preferido 1510, el terminal de acceso 1520 selecciona el femto-nodo 1510 para establecerse dentro de su área de cobertura.

Un femto-nodo puede estar limitado en algunos aspectos. Por ejemplo, un femto-nodo dado solamente puede proporcionar determinados servicios a determinados terminales de acceso. En despliegues con la denominada asociación restringida (o cerrada), un terminal de acceso dado solamente puede recibir servicio por medio de la red móvil de macro-células y por medio de un conjunto definido de femto-nodos (por ejemplo, los femto-nodos 1510 que residen dentro del domicilio de usuario 1530 correspondiente). En algunas implementaciones, un nodo puede estar limitado a no proporcionar, para al menos un nodo, al menos uno entre: señalización, acceso a datos, registro, radiolocalización o servicio.

En algunos aspectos, un femto-nodo restringido (que también puede denominarse NodoB Doméstico de Grupo Cerrado de abonados) es uno que proporciona servicio a un conjunto dotado restringido de terminales de acceso. Este conjunto puede ampliarse de manera temporal o permanente según sea necesario. En algunos aspectos, un grupo cerrado de abonados ("CSG") puede definirse como el conjunto de puntos de acceso (por ejemplo, femto-nodos) que comparten una lista de control de acceso común de terminales de acceso. Un punto de acceso restringido puede incluir un CSG que permite a múltiples terminales de acceso conectarse al mismo. Un terminal de acceso único puede tener la capacidad de conectarse a múltiples puntos de acceso restringido. Un canal en el que funcionan todos los femto-nodos (o todos los femto-nodos restringidos) en una región puede denominarse un femto-canal.

Por lo tanto, pueden existir varias relaciones entre un femto-nodo dado y un terminal de acceso dado. Por ejemplo, desde la perspectiva de un terminal de acceso, un femto-nodo abierto puede referirse a un femto-nodo sin ninguna asociación restringida (por ejemplo, el femto-nodo permite el acceso a cualquier terminal de acceso). Un femto-nodo restringido puede referirse a un femto-nodo que está restringido de alguna manera (por ejemplo, restringido para la asociación y/o el registro). Un femto-nodo doméstico puede referirse a un femto-nodo al cual el terminal de acceso está autorizado a acceder y en el que puede realizar operaciones (por ejemplo, se proporciona un acceso permanente para un conjunto definido de uno o más terminales de acceso). Un femto-nodo invitado puede referirse a un femto-nodo al que un terminal de acceso puede acceder, o con el que puede operar, temporalmente. Un femto-nodo foráneo puede referirse a un femto-nodo al que el terminal de acceso no puede acceder, ni con el que puede operar, excepto, quizá, en situaciones de emergencia (por ejemplo, llamadas al 112).

Desde la perspectiva de un femto-nodo restringido, un terminal de acceso doméstico puede referirse a un terminal de acceso que está autorizado para acceder al femto-nodo restringido (por ejemplo, el terminal de acceso tiene acceso permanente al femto-nodo). Un terminal de acceso invitado puede referirse a un terminal de acceso con acceso temporal al femto-nodo restringido (por ejemplo, limitado en base a una fecha límite, al tiempo de uso, a los octetos, al cómputo de conexiones o a algún, o algunos, otro(s) criterio(s)). Un terminal de acceso foráneo puede referirse a un terminal de acceso que no tiene permiso para acceder al femto-nodo restringido, excepto quizá en situaciones de emergencia, por ejemplo, tales como llamadas al 112 (por ejemplo, un terminal de acceso que no tiene las credenciales o permisos para registrarse en el femto-nodo restringido).

Por comodidad, la divulgación del presente documento describe diversa funcionalidad en el contexto de un femto-nodo. Sin embargo, debe apreciarse que un pico-nodo puede proporcionar la misma funcionalidad, u otra similar,

para un área de cobertura más grande. Por ejemplo, un pico-nodo puede estar restringido, un pico-nodo doméstico puede estar definido para un terminal de acceso dado, etc.

Un sistema de comunicación inalámbrica de acceso múltiple puede prestar soporte simultáneamente a la comunicación para múltiples terminales de acceso inalámbrico. Como se ha mencionado anteriormente, cada terminal puede comunicarse con una o más estaciones base mediante transmisiones en los enlaces directo e inverso. El enlace directo (o enlace descendente) se refiere al enlace de comunicación desde las estaciones base hasta los terminales, y el enlace inverso (o enlace ascendente) se refiere al enlace de comunicación desde los terminales hasta las estaciones base. Este enlace de comunicación puede establecerse mediante un sistema de única entrada y única salida, un sistema de múltiples entradas y múltiples salidas ("MIMO") o algún otro tipo de sistema.

Un sistema de MIMO utiliza múltiples (NT) antenas de transmisión y múltiples (NR) antenas de recepción para la transmisión de datos. Un canal de MIMO formado por las NT antenas de transmisión y las NR antenas de recepción puede descomponerse en NS canales independientes, que también se denominan canales espaciales, donde NS ≤ min {NT, NR}. Cada uno de los NS canales independientes corresponde a una dimensión. El sistema de MIMO puede proporcionar un rendimiento mejorado (por ejemplo, un mayor caudal de tráfico y/o una mayor fiabilidad) si se utilizan las dimensiones adicionales creadas por las múltiples antenas de transmisión y de recepción.

Un sistema de MIMO puede dar soporte al dúplex por división del tiempo ("TDD") y al dúplex por división de frecuencia ("FDD"). En un sistema de TDD, las transmisiones en el enlace directo y el enlace inverso están en la misma región de frecuencia, de modo que el principio de reciprocidad permite la estimación del canal de enlace directo a partir del canal de enlace inverso. Esto permite al punto de acceso extraer una ganancia de conformación de haces de transmisión en el enlace directo cuando múltiples antenas están disponibles en el punto de acceso.

Las enseñanzas en el presente documento pueden incorporarse en un nodo (por ejemplo, un dispositivo) que utiliza varios componentes para la comunicación con al menos otro nodo. La FIG. 17 ilustra varios componentes de muestra que pueden utilizarse para facilitar la comunicación entre nodos. Específicamente, la FIG. 17 ilustra un dispositivo inalámbrico 1710 (por ejemplo, un punto de acceso) y un dispositivo inalámbrico 1750 (por ejemplo, un terminal de acceso) de un sistema de MIMO 1700. En el dispositivo 1710, los datos de tráfico para un cierto número de flujos de datos se proporcionan desde un origen de datos 1712 hasta un procesador de datos de transmisión ("TX") 1714.

En algunos aspectos, cada flujo de datos se transmite a través de una respectiva antena de transmisión. El procesador de datos de TX 1714 formatea, codifica y entrelaza los datos de tráfico para cada flujo de datos basándose en un esquema de codificación particular seleccionado para ese flujo de datos, para proporcionar datos codificados.

Los datos codificados para cada flujo de datos pueden multiplexarse con datos piloto utilizando técnicas de OFDM. Los datos piloto son normalmente un patrón de datos conocido que se procesa de manera conocida y que puede utilizarse en el sistema receptor para estimar la respuesta de canal. Los datos piloto multiplexados y los datos codificados para cada flujo de datos se modulan después (por ejemplo, se correlacionan con símbolos) en base a un esquema de modulación particular (por ejemplo, BPSK, QSPK, M-PSK o M-QAM) seleccionado para que ese flujo de datos proporcione símbolos de modulación. La velocidad de transferencia de datos, la codificación y la modulación para cada flujo de datos puede determinarse mediante instrucciones llevadas a cabo por un procesador 1730. Una memoria de datos 1732 puede almacenar el código de programa, datos y otra información utilizada por el procesador 1730 u otros componentes del dispositivo 1710.

Los símbolos de modulación para todos los flujos de datos se proporcionan después a un procesador de MIMO de TX 1720, que puede procesar adicionalmente los símbolos de modulación (por ejemplo, para el OFDM). El procesador de MIMO de TX 1720 proporciona después NT flujos de símbolos de modulación a NT transceptores ("XCVR") 1722A a 1722T. En algunos aspectos, el procesador de MIMO de TX 1720 aplica ponderaciones de conformación de haces a los símbolos de los flujos de datos y a la antena desde la cual se está transmitiendo el símbolo.

Cada transceptor 1722 recibe y procesa un flujo de símbolos respectivo para proporcionar una o más señales analógicas, y acondiciona adicionalmente (por ejemplo, amplifica, filtra y aumenta en frecuencia) las señales analógicas para proporcionar una señal modulada adecuada para su transmisión por el canal de MIMO. Las NT señales moduladas de los transceptores 1722A a 1722T se transmiten después desde las NT antenas 1724A a 1724T, respectivamente.

En el dispositivo 1750, las señales moduladas transmitidas son recibidas por las NR antenas 1752A a 1752R y la señal recibida desde cada antena 1752 se proporciona a un transceptor respectivo ("XCVR") 1754A a 1754R. Cada transceptor 1754 acondiciona (por ejemplo, filtra, amplifica y reduce en frecuencia) una respectiva señal recibida, digitaliza la señal acondicionada para proporcionar muestras y procesa adicionalmente las muestras para proporcionar un correspondiente flujo de símbolos "recibido".

Después, un procesador de datos de recepción (RX) 1760 recibe y procesa los NR flujos de símbolos recibidos desde los NR transceptores 1754 basándose en una técnica particular de procesamiento de receptor para proporcionar NT flujos de símbolos "detectados". Después, el procesador de datos de RX 1760 desmodula, desentrelaza y decodifica cada flujo de símbolos detectado para recuperar los datos de tráfico para el flujo de datos. El procesamiento por el procesador de datos de RX 1760 es complementario al realizado por el procesador de MIMO de TX 1720 y el procesador de datos de TX 1714 del dispositivo 1710.

Un procesador 1770 determina periódicamente qué matriz de pre-codificación utilizar (lo que se expone posteriormente). El procesador 1770 formula un mensaje de enlace inverso que comprende una parte de índice de matriz y una parte de valor de rango. Una memoria de datos 1772 puede almacenar el código de programa, datos y otra información utilizada por el procesador 1770 u otros componentes del dispositivo 1750.

El mensaje de enlace inverso puede comprender varios tipos de información relacionada con el enlace de comunicaciones y/o con el flujo de datos recibido. El mensaje de enlace inverso se procesa a continuación mediante un procesador de datos de TX 1738, que también recibe datos de tráfico para un cierto número de flujos de datos desde un origen de datos 1736, se modula por un modulador 1780, se acondiciona por los transceptores 1754A a 1754R y se transmite de nuevo al dispositivo 1710.

En el dispositivo 1710, las señales moduladas del dispositivo 1750 son recibidas por las antenas 1724, acondicionadas por los transceptores 1722, desmoduladas por un demodulador (“DEMOD”) 1740 y procesadas por un procesador de datos de RX 1742 para extraer el mensaje de enlace inverso transmitido por el dispositivo 1750. Después, el procesador 1730 determina qué matriz de pre-codificación utilizar para determinar las ponderaciones de conformación de haces y después procesa el mensaje extraído.

La FIG. 17 también ilustra que los componentes de comunicación pueden incluir uno o más componentes que realizan operaciones de control de acceso, como se indica en el presente documento. Por ejemplo, un componente de control de acceso 1790 puede actuar conjuntamente con el procesador 1730 y/o con otros componentes del dispositivo 1710 para enviar/recibir señales a/desde otro dispositivo (por ejemplo, el dispositivo 1750), como se describe en el presente documento. Asimismo, un componente de control de acceso 1792 puede actuar conjuntamente con el procesador 1770 y/o con otros componentes del dispositivo 1750 para enviar/recibir señales a/desde otro dispositivo (por ejemplo, el dispositivo 1710). Debería apreciarse que, para cada dispositivo 1710 y 1750, la funcionalidad de dos o más de los componentes descritos puede proporcionarse por un único componente. Por ejemplo, un único componente de procesamiento puede proporcionar la funcionalidad del componente de control de acceso 1790 y del procesador 1730, y un único componente de procesamiento puede proporcionar la funcionalidad del componente de control de acceso 1792 y del procesador 1770.

Las enseñanzas en el presente documento pueden incorporarse en varios tipos de sistemas de comunicación y/o de componentes de sistema. En algunos aspectos, las enseñanzas en el presente documento pueden utilizarse en un sistema de acceso múltiple capaz de prestar soporte a comunicaciones con múltiples usuarios, compartiendo los recursos de sistema disponibles (por ejemplo, especificando uno o más entre el ancho de banda, la potencia de transmisión, la codificación, el entrelazado, etc.). Por ejemplo, las enseñanzas en el presente documento pueden aplicarse a una cualquiera, o a combinaciones, de las siguientes tecnologías: Sistemas de acceso múltiple por división de código ("CDMA"), CDMA de múltiples portadoras ("MCCDMA"), CDMA de banda ancha ("W-CDMA"), sistemas de acceso por paquetes de alta velocidad ("HSPA", "HSPA+"), sistemas de acceso múltiple por división de tiempo ("TDMA"), sistemas de acceso múltiple por división de frecuencia ("FDMA"), sistemas de FDMA de única portadora ("SC-FDMA"), sistemas de acceso múltiple por división de frecuencia ortogonal ("OFDMA") u otras técnicas de acceso múltiple. Un sistema de comunicaciones inalámbricas que utiliza las enseñanzas en el presente documento puede diseñarse para implementar una o más normas, tales como IS-95, cdma2000, IS- 856, W-CDMA, TDSCDMA y otras normas. Una red de CDMA puede implementar una tecnología de radio tal como el acceso por radio terrestre universal ("UTRA"), cdma2000 o alguna otra tecnología. El UTRA incluye el W-CDMA y la baja velocidad de chip ("LCR"). La tecnología cdma2000 abarca las normas IS-2000, IS-95 e IS-856. Una red de TDMA puede implementar una tecnología de radio tal como el Sistema Global de Comunicaciones Móviles ("GSM"). Una red de OFDMA puede implementar una tecnología de radio tal como el UTRA Evolucionado ("E-UTRA"), IEEE 802.11, IEEE 802.16, IEEE 802.20, Flash-OFDM□, etc. UTRA, EUTRA y GSM son parte del Sistema Universal de Telecomunicaciones Móviles ("UMTS"). Las enseñanzas en el presente documento pueden implementarse en un sistema de Evolución a Largo Plazo ("LTE") del 3GPP, en un sistema de Banda Ancha Ultra-móvil ("UMB") y en otros tipos de sistemas. La LTE es una versión del UMTS que usa el E-UTRA. Aunque determinados aspectos de la divulgación pueden describirse usando terminología del 3GPP, debe entenderse que las enseñanzas en el presente documento pueden aplicarse a tecnología del 3GPP (Re199, Re15, Re16, Re17) así como a tecnologías del 3GPP2 (IxRTT, 1xEV-DO ReIO, RevA, RevB) y a otras tecnologías.

Las enseñanzas en el presente documento pueden incorporarse en (por ejemplo, implementarse dentro de, o llevarse a cabo por) varios aparatos (por ejemplo, nodos). En algunos aspectos, un nodo (por ejemplo, un nodo inalámbrico) implementado según las enseñanzas en el presente documento puede comprender un punto de acceso o un terminal de acceso.

Por ejemplo, un terminal de acceso puede comprender, implementarse como o denominarse, un equipo de usuario, una estación de abonado, una unidad de abonado, una estación móvil, un móvil, un nodo móvil, una estación remota, un terminal remoto, un terminal de usuario, un agente de usuario, un dispositivo de usuario o usando otra terminología. En algunas implementaciones, un terminal de acceso puede comprender un teléfono celular, un teléfono sin cables, un teléfono de protocolo de inicio de sesión ("SIP"), una estación de bucle local inalámbrico ("WLL"), un asistente digital personal ("PDA"), un dispositivo manual con capacidad de conexión inalámbrica o algún otro dispositivo de procesamiento adecuado conectado a un módem inalámbrico. Por consiguiente, uno o más aspectos dados a conocer en el presente documento pueden incorporarse en un teléfono (por ejemplo, un teléfono celular o un teléfono inteligente), un ordenador (por ejemplo, un ordenador portátil), un dispositivo de comunicaciones portátil, un dispositivo informático portátil (por ejemplo, un asistente de datos personal), un dispositivo de entretenimiento (por ejemplo, un dispositivo de música, un dispositivo de vídeo o una radio por satélite), un dispositivo del sistema de localización global o cualquier otro dispositivo adecuado que esté configurado para comunicarse a través de un medio inalámbrico.

Un punto de acceso puede comprender, implementarse como o denominarse, un NodoB, un eNodoB, un controlador de red de radio ("RNC"), una estación base ("BS"), una estación base de radio ("RBS"), un controlador de estación base ("BSC"), una estación transceptora base ("BTS"), una función transceptora ("TF"), un transceptor de radio, un encaminador de radio, un conjunto de servicios básicos ("BSS"), un conjunto de servicios extendidos ("ESS") o usando otra terminología similar.

En algunos aspectos, un nodo (por ejemplo, un punto de acceso) puede comprender un nodo de acceso para un sistema de comunicación. Tal nodo de acceso puede proporcionar, por ejemplo, conectividad para o con una red (por ejemplo, una red de área amplia tal como Internet o una red celular) mediante un enlace de comunicación cableado o inalámbrico a la red. Por consiguiente, el nodo de acceso puede permitir que otro nodo (por ejemplo, un terminal de acceso) acceda a una red, o alguna otra funcionalidad. Además, debería apreciarse que uno de los nodos, o ambos, pueden ser portátiles o, en algunos casos, relativamente no portátiles.

Además, debería apreciarse que un nodo inalámbrico puede ser capaz de transmitir y/o de recibir información de manera no inalámbrica (por ejemplo, mediante una conexión cableada). Por lo tanto, un receptor y un transmisor, como los expuestos en el presente documento, pueden incluir componentes adecuados de interfaz de comunicación (por ejemplo, componentes de interfaz eléctrica u óptica) para comunicarse a través de un medio no inalámbrico.

Un nodo inalámbrico puede comunicarse mediante uno o más enlaces de comunicación inalámbrica que están basados en, o que dan soporte de otra forma a, cualquier tecnología adecuada de comunicación inalámbrica. Por ejemplo, en algunos aspectos, un nodo inalámbrico puede asociarse a una red. En algunos aspectos, la red puede comprender una red de área local o una red de área amplia. Un dispositivo inalámbrico puede dar soporte a, o usar de otro modo, una o más entre diversas tecnologías, protocolos o normas de comunicación inalámbrica, tales como los expuestos en el presente documento (por ejemplo, CDMA, TDMA, OFDM, OFDMA, WiMAX, Wi-Fi, etc.). De manera similar, un nodo inalámbrico puede dar soporte a, o usar de otro modo, uno o más entre diversos esquemas correspondientes de modulación o multiplexado. Por lo tanto, un nodo inalámbrico puede incluir componentes adecuados (por ejemplo, interfaces aéreas) para establecer y comunicarse mediante uno o más enlaces de comunicación inalámbrica, usando las anteriores u otras tecnologías de comunicación inalámbrica. Por ejemplo, un nodo inalámbrico puede comprender un transceptor inalámbrico con componentes asociados de transmisión y recepción, que pueden incluir varios componentes (por ejemplo, generadores de señales y procesadores de señales) que facilitan la comunicación a través de un medio inalámbrico.

Los componentes descritos en el presente documento pueden implementarse de múltiples maneras. En referencia a las FIG. 18 a 28, los aparatos 1800, 1900, 2000, 2100, 2200, 2300, 2400, 2500, 2600, 2700 y 2800 están representados como una serie de bloques funcionales interrelacionados. En algunos aspectos, la funcionalidad de estos bloques puede implementarse como un sistema de procesamiento que incluye uno o más componentes de procesamiento. En algunos aspectos, la funcionalidad de estos bloques puede implementarse usando, por ejemplo, al menos una parte de uno o más circuitos integrados (por ejemplo, un ASIC). Como se ha expuesto en el presente documento, un circuito integrado puede incluir un procesador, software, otros componentes relacionados o alguna combinación de los mismos. La funcionalidad de estos bloques también puede implementarse de diferente manera a como se enseña en el presente documento. En algunos aspectos, uno o más de los bloques de trazo discontinuo de las FIGs.

Los aparatos 1800, 1900, 2000, 2100, 2200, 2300, 2400, 2500, 2600, 2700 y 2800 pueden incluir uno o más módulos que pueden realizar una o más de las funciones descritas anteriormente con respecto a las diversas figuras. Por ejemplo, un medio de recepción / envío 1802 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de determinación de un identificador 1804 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de determinación de servicio permitido 1806 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de recepción 1902 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de envío 1904 puede corresponder, por ejemplo, a un

controlador de acceso, como se expone en este documento. Un medio de determinación de identificador 1906 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de envío 2002 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de recepción 2004 puede corresponder, por ejemplo, aun controlador de comunicación, como se expone en este documento. Un medio de determinación de servicio permitido 2006 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de configuración 2102 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en el presente documento. Un medio de obtención 2104 pueden corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de recepción 2106 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de determinación 2108 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de determinación de identificador 2202 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en este documento. Un medio de envío 2204 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de asignación 2206 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en el presente documento. Un medio de recepción 2302 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en el presente documento. Un medio de transmisión 2304 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de determinación de identificador 2402 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en este documento. Un medio de envío 2404 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de recepción 2502 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de determinación de habilitación de acceso 2504 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento.

Un medio de determinación basado en configuración 2506 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de mantenimiento de listas 2508 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de configuración 2802 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en el presente documento. Un medio de transmisión 2604 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de recepción 2606 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de envío 2608 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en el presente documento. Un medio de definición 2610 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en el presente documento. Un medio de monitorización 2702 puede corresponder, por ejemplo, a un receptor, como se expone en este documento. Un medio de recepción de baliza 2704 puede corresponder, por ejemplo, a un receptor, como se expone en este documento. Un medio de envío 2706 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de recepción de listas de itinerancia 2708 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en este documento. Un medio de configuración 2802 puede corresponder, por ejemplo, a un controlador de dotación, como se expone en el presente documento. Un medio de recepción de baliza 2804 puede corresponder, por ejemplo, a un receptor, como se expone en este documento. Un medio de envío 2806 puede corresponder, por ejemplo, a un controlador de comunicación, como se expone en este documento. Un medio de recepción de autorización 2808 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de solicitación 2810 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento. Un medio de exhibición 2812 puede corresponder, por ejemplo, a un controlador de acceso, como se expone en este documento.

Debería entenderse que cualquier referencia a un elemento en el presente documento, utilizando una designación tal como "primero", "segundo", etc., no limita, por lo general, la cantidad o el orden de esos elementos. En cambio, estas designaciones pueden usarse en el presente documento como un procedimiento conveniente para distinguir entre dos o más elementos o instancias de un elemento. Por lo tanto, una referencia a elementos primero y segundo no significa que solamente puedan usarse allí dos elementos, o que el primer elemento deba preceder al segundo elemento de alguna forma. Además, a menos que se indique lo contrario, un conjunto de elementos puede comprender uno o más elementos.

Los expertos en la técnica entenderán que la información y las señales pueden representarse usando cualquiera entre una variedad de tecnologías y de técnicas diferentes. Por ejemplo, los datos, las instrucciones, los comandos, la información, las señales, los bits, los símbolos y los chips que pueden haber sido mencionados a lo largo de la descripción anterior, pueden representarse mediante tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos, o cualquier combinación de los mismos.

Los expertos en la técnica apreciarán además que cualquiera de los diversos bloques lógicos, módulos, procesadores, medios, circuitos y etapas de algoritmo ilustrativos descritos en relación con los aspectos divulgados en el presente documento pueden implementarse como hardware electrónico (por ejemplo, una implementación digital, una implementación analógica o una combinación de las dos, que puede diseñarse utilizando codificación fuente o alguna otra técnica), como varias formas de código de programa o de diseño que incluyen instrucciones (que pueden denominarse en el presente documento, por comodidad, “software” o "módulo de software”), o como combinaciones de lo anterior. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente

se han descrito diversos componentes, bloques, módulos, circuitos y etapas ilustrativos en lo que respecta generalmente a su funcionalidad. Si tal funcionalidad se implementa como hardware o software depende de la aplicación particular y de las limitaciones de diseño impuestas sobre todo el sistema. Los expertos en la técnica pueden implementar la funcionalidad descrita de diferentes maneras para cada aplicación particular, pero no debe interpretarse que tales decisiones de implementación suponen una desviación del alcance de la presente divulgación.

Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con los aspectos divulgados en el presente documento pueden implementarse dentro de, o ser llevados a cabo por, un circuito integrado ("CI"), un terminal de acceso o un punto de acceso. El CI puede comprender un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado específico de la aplicación (ASIC), una formación de compuertas programables en el terreno (FPGA) u otro dispositivo de lógica programable, lógica de compuertas discretas o de transistores, componentes de hardware discretos, componentes eléctricos, componentes ópticos, componentes mecánicos o cualquier combinación de los mismos diseñada para llevar a cabo las funciones descritas en el presente documento, y puede ejecutar códigos o instrucciones que residan en el CI, fuera del CI o en ambos casos. Un procesador de propósito general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador, controlador, micro-controlador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

Debe entenderse que cualquier orden específico o jerarquía de etapas en cualquier proceso divulgado es un ejemplo de un enfoque de muestra. En base a las preferencias de diseño, debe entenderse que el orden o jerarquía específicos de las etapas en los procesos puede reorganizarse, manteniéndose a la vez dentro del alcance de la presente divulgación. Las reivindicaciones de procedimiento adjuntas presentan elementos de las diversas etapas en un orden a modo de muestra, y no están concebidas para limitarse al orden o jerarquía específicos presentados.

Las funciones descritas pueden implementarse en hardware, software, firmware o cualquier combinación de los mismos. Si se implementan en software, las funciones pueden almacenarse o transmitirse como una o más instrucciones o códigos en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informáticos como medios de comunicación, incluyendo cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que pueda accederse mediante un ordenador. A modo de ejemplo, y no de manera limitativa, tales medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para transportar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Además, cualquier conexión recibe adecuadamente la denominación de medios legibles por ordenador. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota, usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas tales como infrarrojos, radio y microondas, se incluyen en la definición de medio. Los discos, tal como se usan en el presente documento, incluyen el disco compacto (CD), el disco de láser, el disco óptico, el disco versátil digital (DVD), el disco flexible y el disco Blu-ray, donde algunos discos normalmente reproducen datos de manera magnética, mientras que otros discos reproducen los datos de manera óptica con láser. Las combinaciones de lo anterior también deberían incluirse dentro del alcance de los medios legibles por ordenador. De forma resumida, debería apreciarse que un medio legible por ordenador puede implementarse en cualquier producto adecuado de programa informático.

La anterior descripción de los aspectos divulgados se proporciona para permitir que cualquier experto en la técnica realice o use la presente divulgación. Diversas modificaciones de estos aspectos resultarán inmediatamente evidentes a los expertos en la técnica. Por lo tanto, la presente divulgación no pretende limitarse a los aspectos mostrados en el presente documento.

REIVINDICACIONES

1. Un procedimiento de comunicación realizado por un nodo de red (110), que comprende:

la recepción de una solicitud de un identificador al recibir un identificador propuesto de un conjunto de al menos un punto de acceso (102, 104) que está configurado para proporcionar al menos un servicio solamente a un conjunto definido de terminales de acceso plurales (106, 108),

en el que el identificador propuesto está pensado para identificar de forma única el conjunto de al menos un punto de acceso dentro de una red de operador y ser difundido por el aire por el conjunto de al menos un punto de acceso (102, 104);

determinar si el identificador propuesto ya está en uso por otro conjunto de al menos un punto de acceso (102, 104) dentro de la red de operador;

si el identificador propuesto ya está en uso, seleccionar otro identificador; y

enviar el identificador seleccionado a cada punto de acceso (102, 104) en el conjunto de al menos un punto de acceso (102, 104).

2. El procedimiento de la reivindicación 1, en el que:

el identificador propuesto comprende un identificador de red; y

la red comprende un dominio de operador celular.

3. El procedimiento de la reivindicación 2, en el que el conjunto de al menos un punto de acceso comprende una pluralidad de puntos de acceso que están asociados a un grupo cerrado de abonados común.

4. El procedimiento de la reivindicación 2, en el que el identificador propuesto está basado en texto.

5. El procedimiento de la reivindicación 2, en el que cada punto de acceso del conjunto de al menos un punto de acceso está restringido a no proporcionar, para al menos otro terminal de acceso, por lo menos uno del grupo que consiste en: señalización, acceso a datos, registro y servicio.

6. El procedimiento de la reivindicación 1, que comprende además la asignación de un identificador de dispositivo único para cada punto de acceso del conjunto de al menos un punto de acceso.

7. El procedimiento de la reivindicación 1, en el que cada punto de acceso del conjunto de al menos un punto de acceso ofrece diferentes servicios, para el conjunto de terminales de acceso plurales, que para al menos otro terminal de acceso.

8. El procedimiento de la reivindicación 1, que además comprende dotar al punto de acceso de uno o más identificadores asociados a cada terminal de acceso al que se permita acceder al punto de acceso.

9. Un nodo de red (110), que comprende:

medios para recibir una solicitud de un identificador al recibir un identificador propuesto de un conjunto de al menos un punto de acceso (102, 104) que está configurado para proporcionar al menos un servicio solamente a un conjunto definido de terminales de acceso plurales (106, 108), en el que el identificador propuesto está pensado para identificar de forma única el conjunto de al menos un punto de acceso dentro de una red de operador y ser difundido por el aire por el conjunto de al menos un punto de acceso (102, 104);

medios para determinar si el identificador propuesto ya está en uso por otro conjunto de al menos un punto de acceso (102, 104) dentro de la red de operador;

si el identificador propuesto ya está en uso, medios para seleccionar otro identificador; y

medios para enviar el identificador seleccionado en respuesta a la solicitud de cada punto de acceso (102, 104) en el conjunto de al menos un punto de acceso.

10. Un procedimiento de comunicación, realizado por un conjunto de al menos un punto de acceso (102, 104), en el que cada punto de acceso (102, 104) del conjunto está configurado para proporcionar al menos un servicio solamente a un conjunto definido de terminales de acceso plurales (106, 108), que comprende:

determinar un identificador propuesto y enviar una solicitud de un identificador al enviar el identificador propuesto a un nodo de red (110), en el que el identificador propuesto está pensado para identificar de forma única el conjunto de al menos un punto de acceso dentro de una red de operador y difundirlo; recibir un identificador seleccionado; y

difundir (410) el identificador seleccionado por el aire.

11. El procedimiento de la reivindicación 10, en el que el identificador se recibe en respuesta a una solicitud del identificador.

12. Un conjunto de al menos un punto de acceso (102, 104), en el que cada punto de acceso (102, 104) del conjunto está configurado para proporcionar al menos un servicio solamente a un conjunto definido de terminales de acceso plurales (106, 108), que comprende:

medios para determinar un identificador propuesto y enviar una solicitud de un identificador al enviar el identificador propuesto a un nodo de red (110), en el que el identificador propuesto está pensado para identificar de forma única el conjunto de al menos un punto de acceso dentro de una red de operador y difundirlo;

medios para recibir un identificador seleccionado para el conjunto de al menos un punto de acceso,

medios para difundir (410) el identificador seleccionado por el aire.

13. Producto de programa informático que comprende:

un medio legible por ordenador que comprende códigos para hacer que un ordenador realice las etapas de uno cualquiera de los procedimientos de las reivindicaciones 1 a 8, 10 u 11.

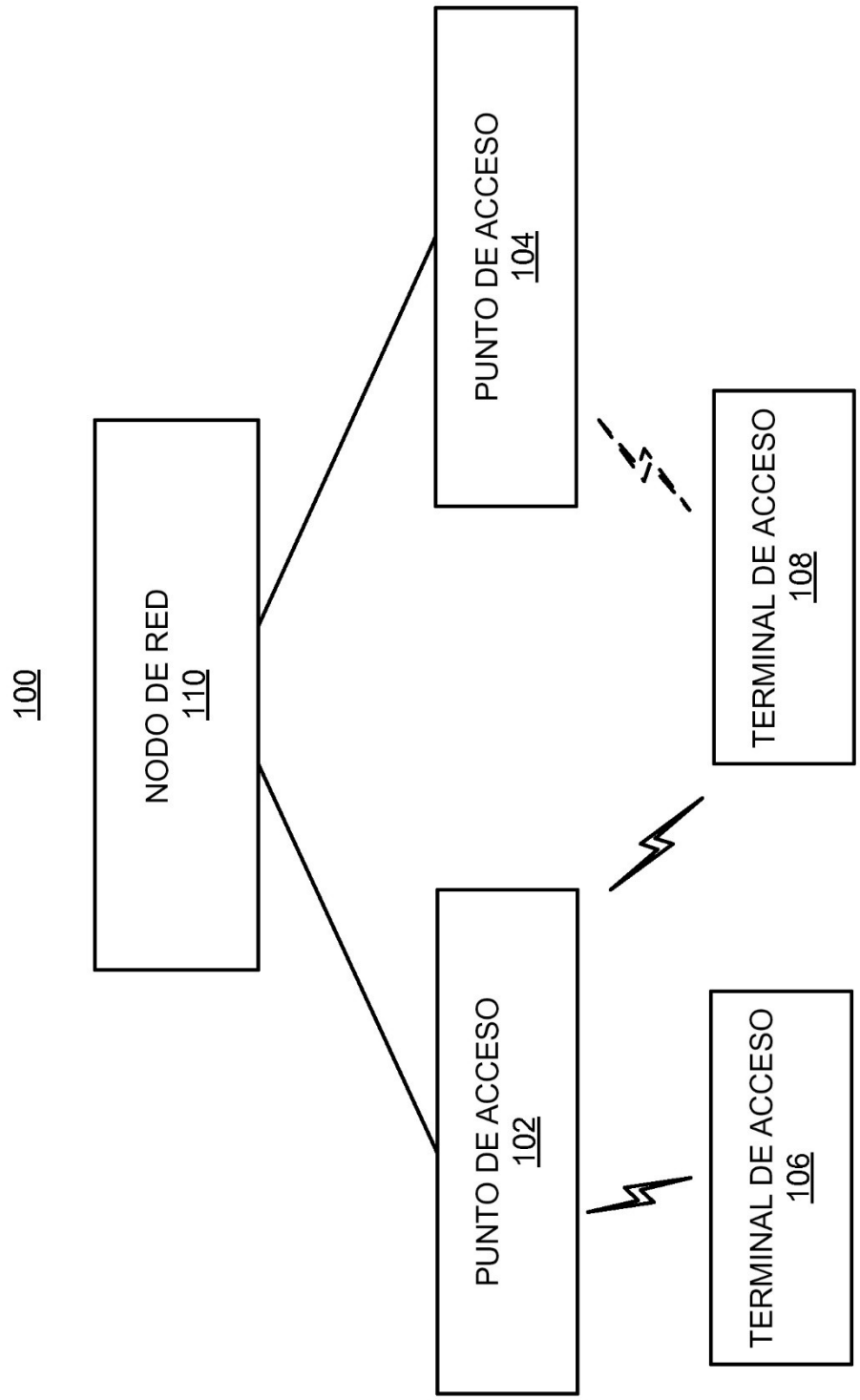
100
NODO DE RED
110
PUNTO DE ACCESO
104
PUNTO DE ACCESO
102
TERMINAL DE ACCESO
108
TERMINAL DE ACCESO
106

FIG. 1

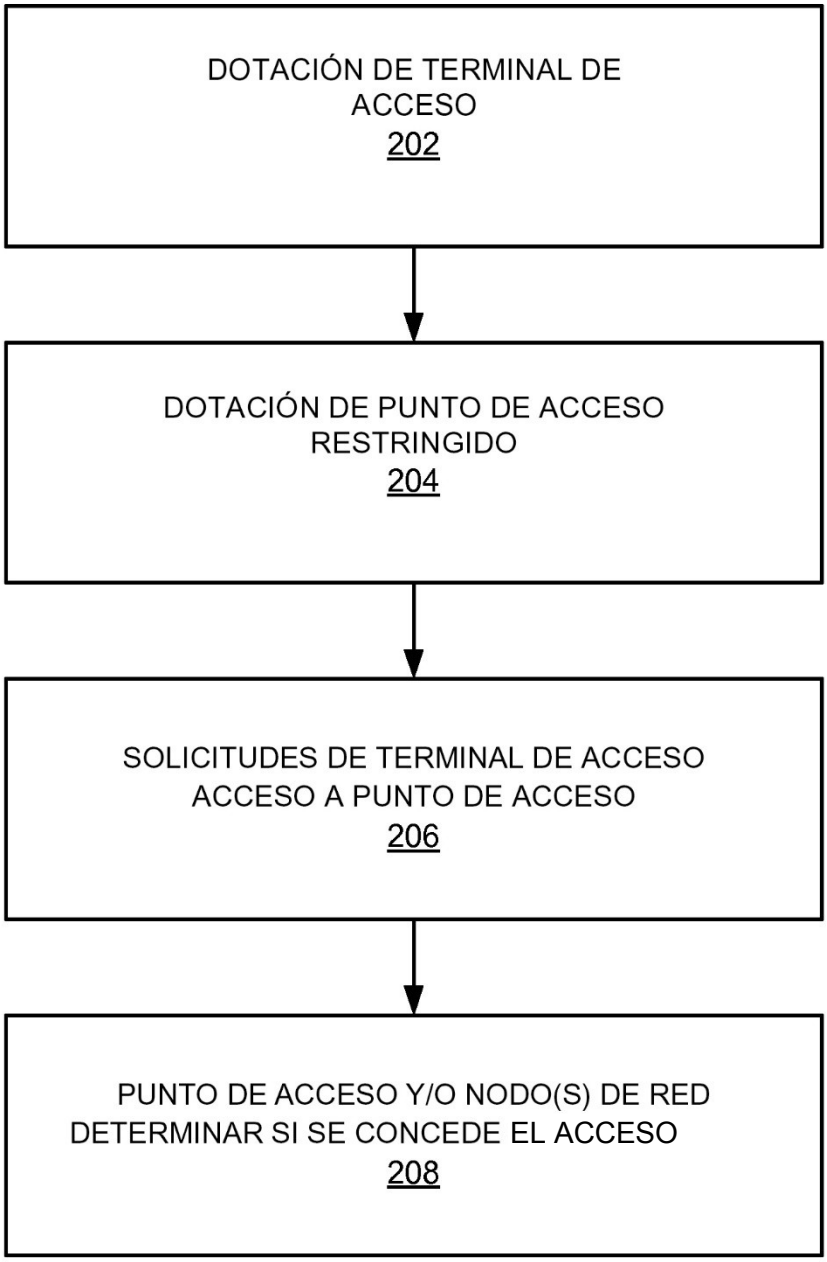
DOTACIÓN DE TERMINAL DE ACCESO
202
DOTACIÓN DE PUNTO DE ACCESO RESTRINGIDO
204
SOLICITUDES DE TERMINAL DE ACCESO ACCESO A PUNTO DE ACCESO
206
PUNTO DE ACCESO Y/O NODO(S) DE RED DETERMINAR SI SE CONCEDE EL ACCESO
208

FIG. 2

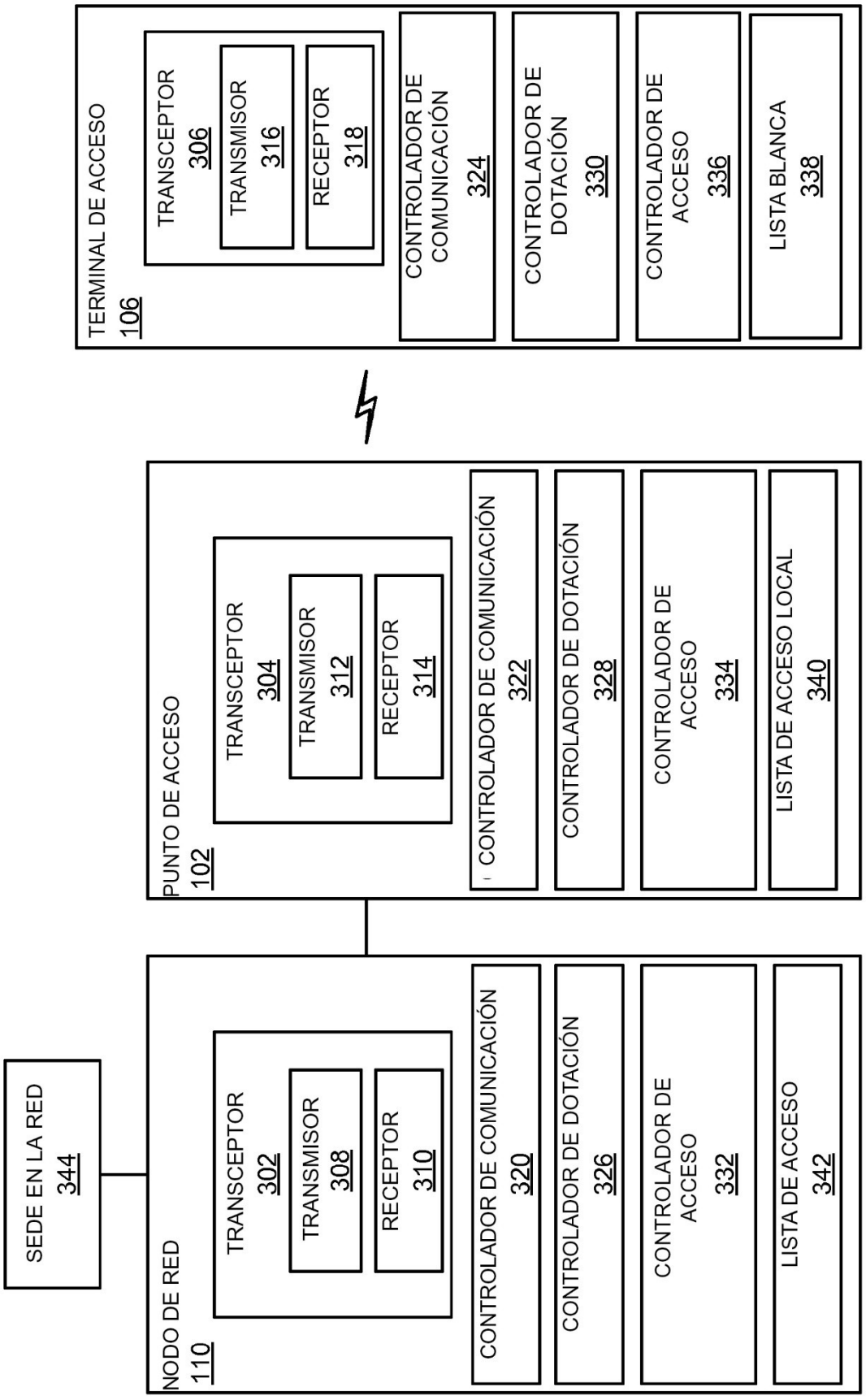
300
SEDE EN LA RED
344
NODO DE RED
110
TRANSCEPTOR
302
TRANSMISOR
308
RECEPTOR
310
CONTROLADOR DE COMUNICACIÓN
320
CONTROLADOR DE DOTACIÓN
326
CONTROLADOR DE ACCESO
332
LISTA DE ACCESO
342
PUNTO DE ACCESO
102
TRANSCEPTOR
304
TRANSMISOR
312
RECEPTOR
314
CONTROLADOR DE COMUNICACIÓN
322
CONTROLADOR DE DOTACIÓN
328
CONTROLADOR DE ACCESO
334
LISTA DE ACCESO LOCAL
340
TERMINAL DE ACCESO
106
TRANSCEPTOR
306
TRANSMISOR
316
RECEPTOR
318
CONTROLADOR DE COMUNICACIÓN
324
CONTROLADOR DE DOTACIÓN
330
CONTROLADOR DE ACCESO
336
LISTA BLANCA
338

FIG. 3

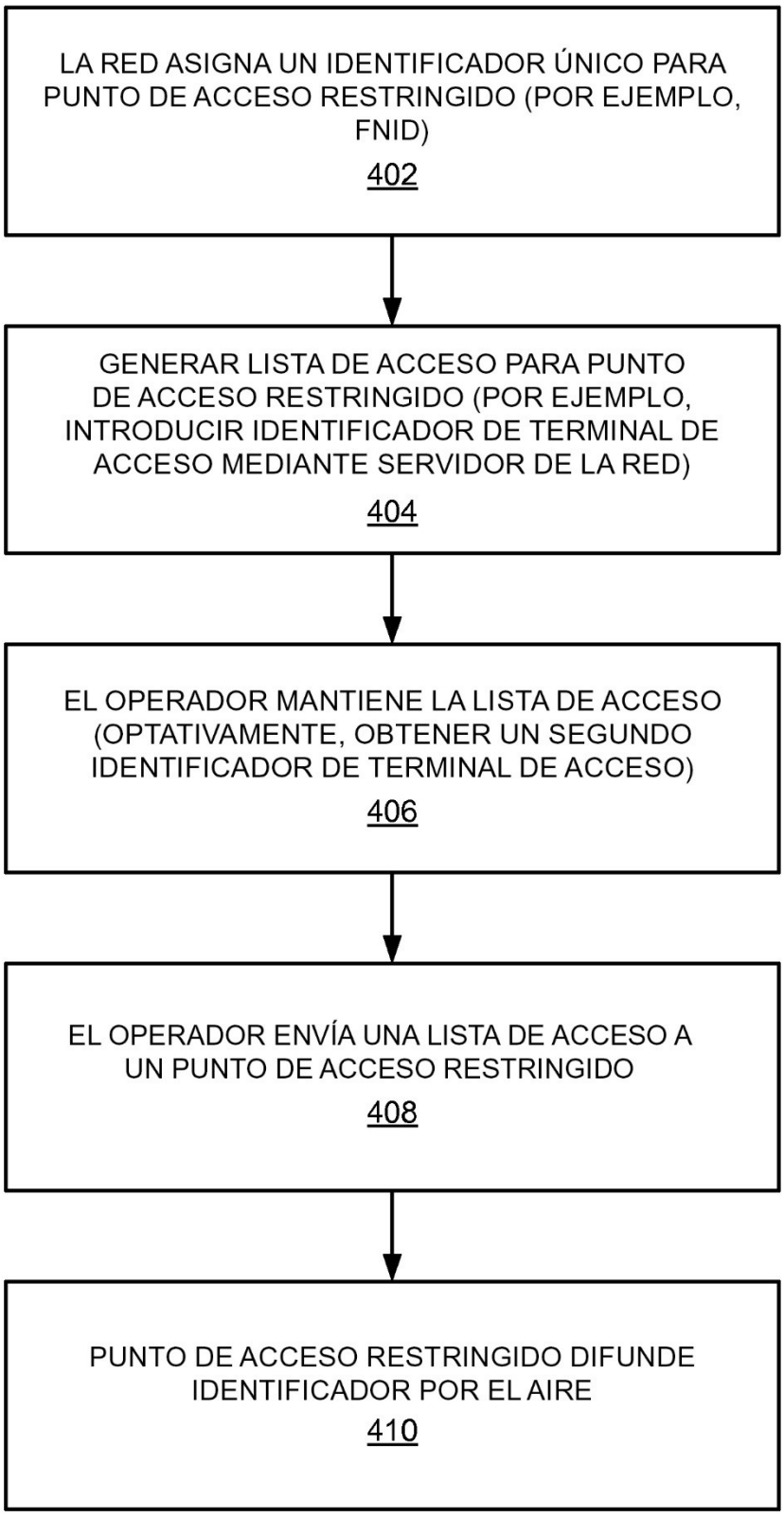
LA RED ASIGNA UN IDENTIFICADOR ÚNICO PARA PUNTO DE ACCESO RESTRINGIDO (POR EJEMPLO, FNID)
402
GENERAR LISTA DE ACCESO PARA PUNTO DE ACCESO RESTRINGIDO (POR EJEMPLO, INTRODUCIR IDENTIFICADOR DE TERMINAL DE ACCESO MEDIANTE SERVIDOR DE LA RED)
404
EL OPERADOR MANTIENE LA LISTA DE ACCESO (OPTATIVAMENTE, OBTENER UN SEGUNDO IDENTIFICADOR DE TERMINAL DE ACCESO)
406
EL OPERADOR ENVÍA UNA LISTA DE ACCESO A UN PUNTO DE ACCESO RESTRINGIDO
408
PUNTO DE ACCESO RESTRINGIDO DIFUNDE IDENTIFICADOR POR EL AIRE
410

FIG. 4

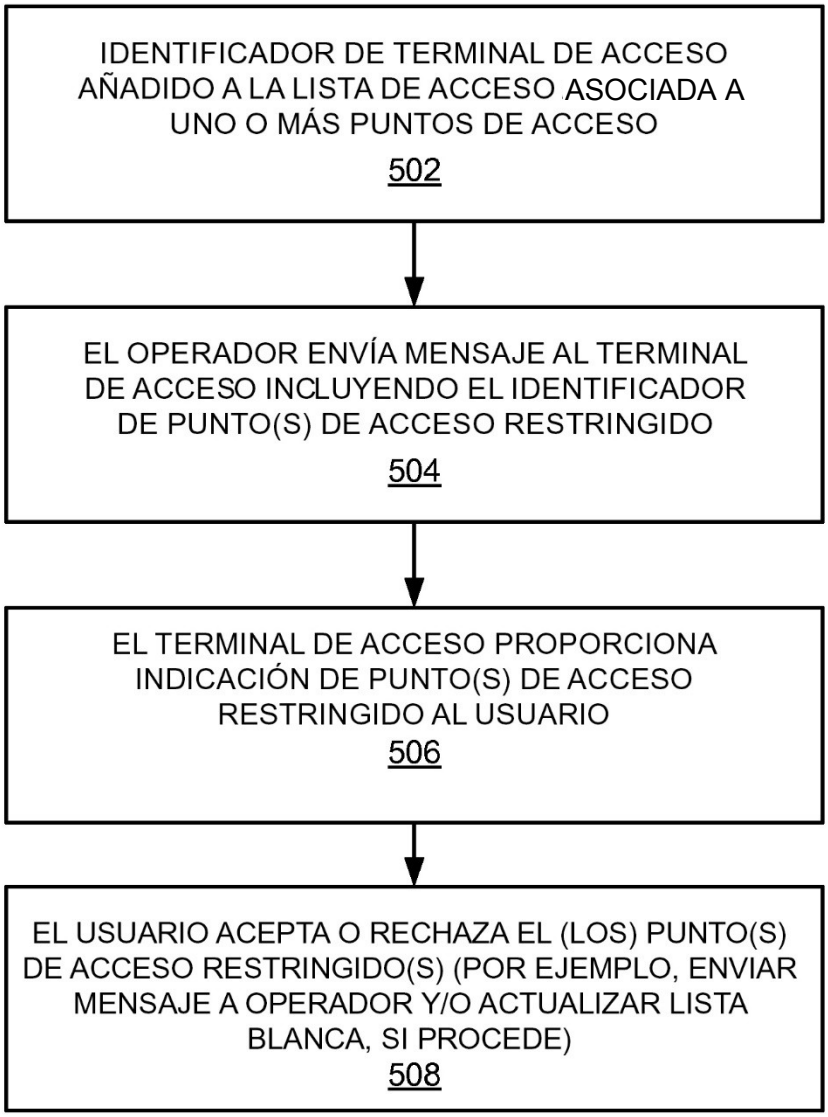
IDENTIFICADOR DE TERMINAL DE ACCESO AÑADIDO A LA LISTA DE ACCESO ASOCIADA A UNO O MÁS PUNTOS DE ACCESO
502
EL OPERADOR ENVÍA MENSAJE AL TERMINAL DE ACCESO INCLUYENDO EL IDENTIFICADOR DE PUNTO(S) DE ACCESO RESTRINGIDO
504
EL TERMINAL DE ACCESO PROPORCIONA INDICACIÓN DE PUNTO(S) DE ACCESO RESTRINGIDO AL USUARIO
506
EL USUARIO ACEPTA O RECHAZA EL (LOS) PUNTO(S) DE ACCESO RESTRINGIDO(S) (POR EJEMPLO, ENVIAR MENSAJE A OPERADOR Y/O ACTUALIZAR LISTA BLANCA, SI PROCEDE)
508

FIG. 5

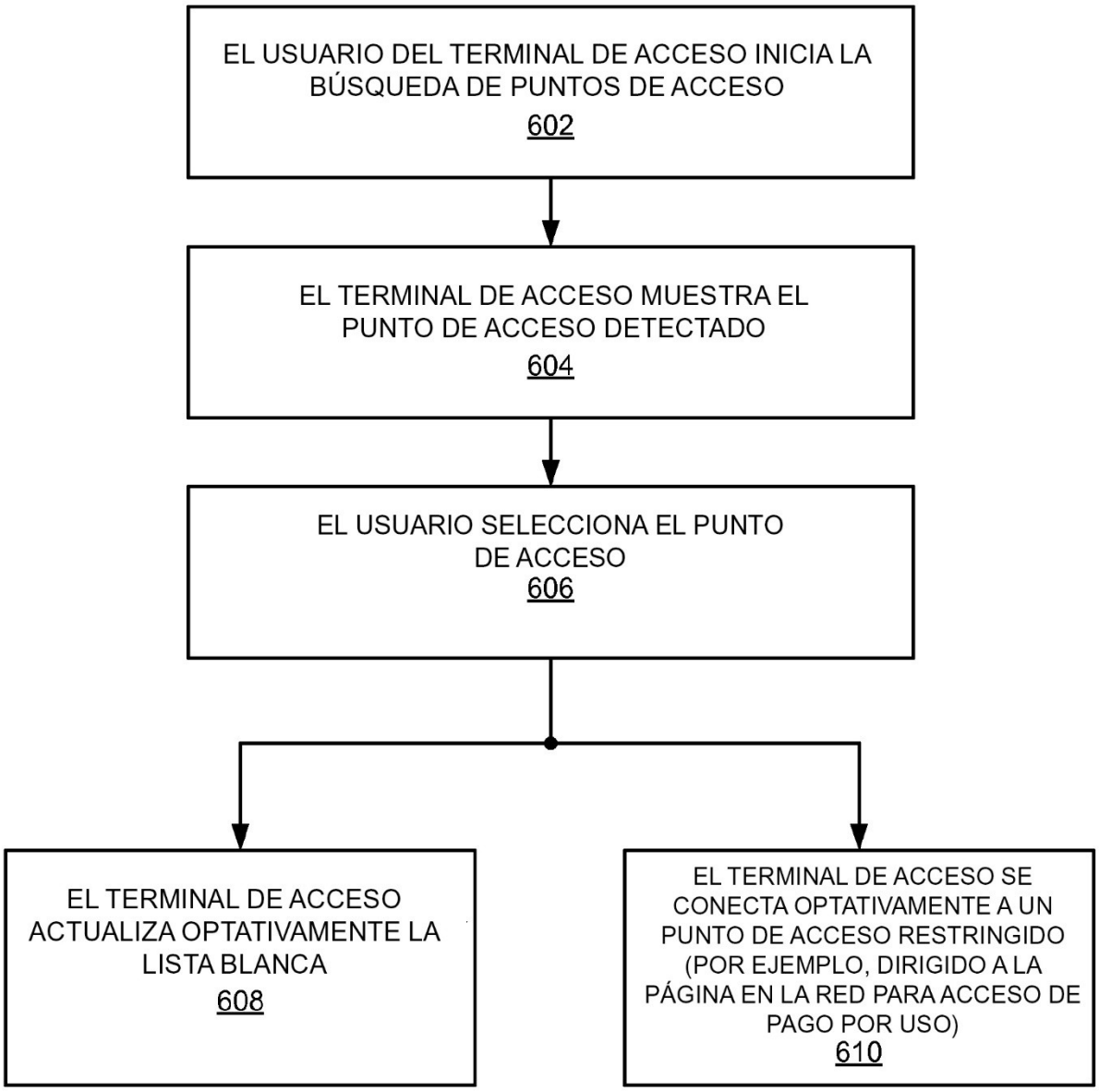
EL USUARIO DEL TERMINAL DE ACCESO INICIA LA BÚSQUEDA DE PUNTOS DE ACCESO
602
EL TERMINAL DE ACCESO MUESTRA EL PUNTO DE ACCESO DETECTADO
604
EL USUARIO SELECCIONA EL PUNTO DE ACCESO
606
EL TERMINAL DE ACCESO ACTUALIZA OPTATIVAMENTE LA LISTA BLANCA
608
EL TERMINAL DE ACCESO SE CONECTA OPTATIVAMENTE A UN PUNTO DE ACCESO RESTRINGIDO (POR EJEMPLO, DIRIGIDO A LA PÁGINA EN LA RED PARA ACCESO DE PAGO POR USO)
610

FIG. 6

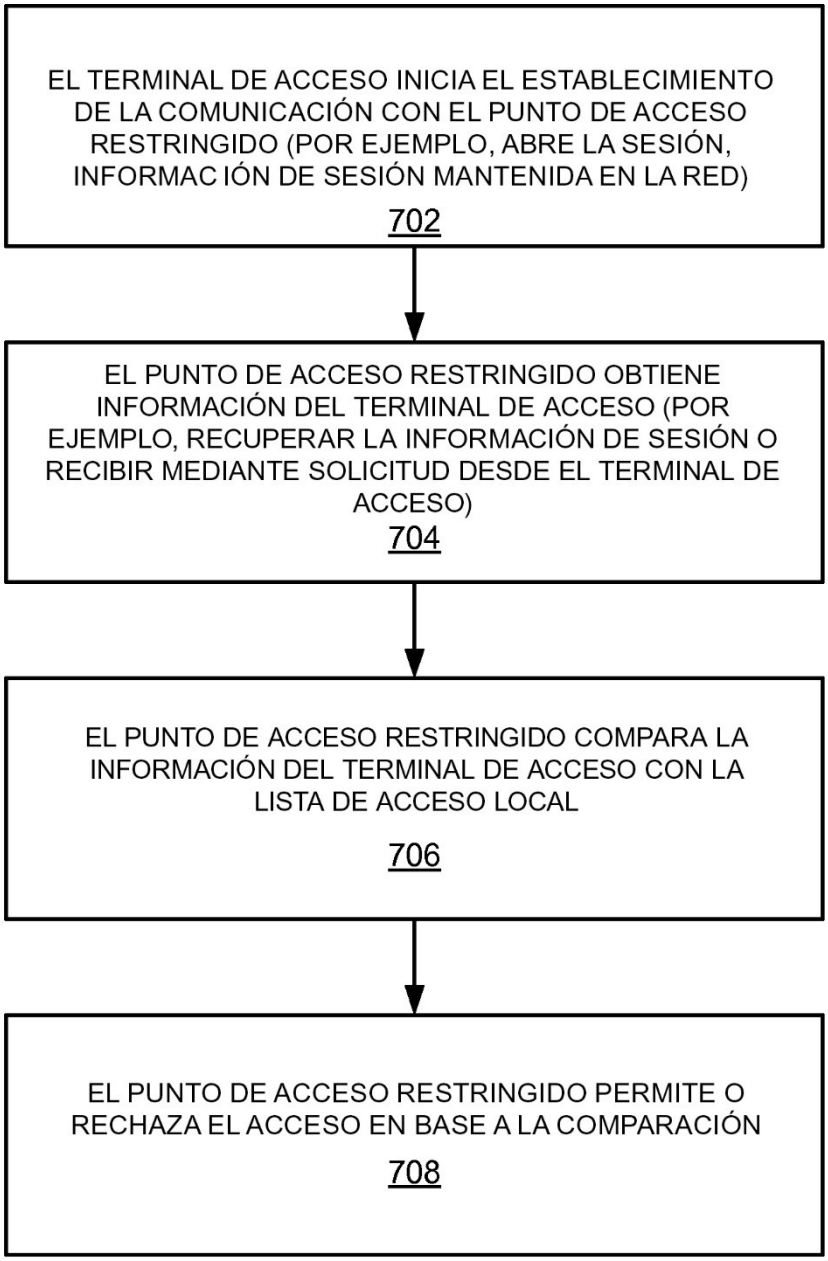
EL TERMINAL DE ACCESO INICIA EL ESTABLECIMIENTO DE LA COMUNICACIÓN CON EL PUNTO DE ACCESO RESTRINGIDO (POR EJEMPLO, ABRE LA SESIÓN, INFORMAC IÓN DE SESIÓN MANTENIDA EN LA RED)
702
EL PUNTO DE ACCESO RESTRINGIDO OBTIENE INFORMACIÓN DEL TERMINAL DE ACCESO (POR EJEMPLO, RECUPERAR LA INFORMACIÓN DE SESIÓN O RECIBIR MEDIANTE SOLICITUD DESDE EL TERMINAL DE ACCESO)
704
EL PUNTO DE ACCESO RESTRINGIDO COMPARA LA INFORMACIÓN DEL TERMINAL DE ACCESO CON LA LISTA DE ACCESO LOCAL
706
EL PUNTO DE ACCESO RESTRINGIDO PERMITE O RECHAZA EL ACCESO EN BASE A LA COMPARACIÓN
708

FIG. 7

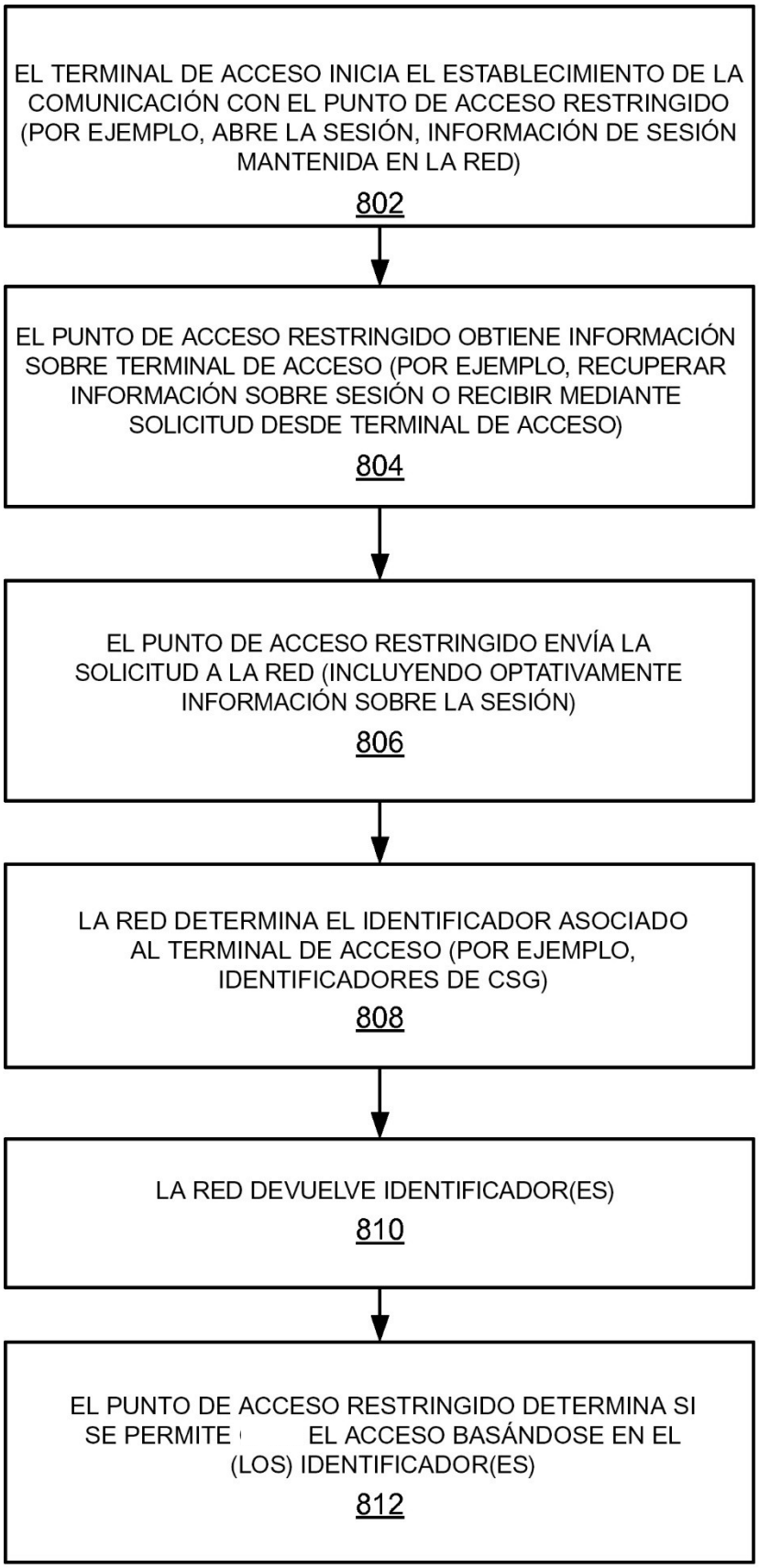
EL TERMINAL DE ACCESO INICIA EL ESTABLECIMIENTO DE LA COMUNICACIÓN CON EL PUNTO DE ACCESO RESTRINGIDO (POR EJEMPLO, ABRE LA SESIÓN, INFORMACIÓN DE SESIÓN MANTENIDA EN LA RED)
802
EL PUNTO DE ACCESO RESTRINGIDO OBTIENE INFORMACIÓN SOBRE TERMINAL DE ACCESO (POR EJEMPLO, RECUPERAR INFORMACIÓN SOBRE SESIÓN O RECIBIR MEDIANTE SOLICITUD DESDE TERMINAL DE ACCESO)
804
EL PUNTO DE ACCESO RESTRINGIDO ENVÍA LA SOLICITUD A LA RED (INCLUYENDO OPTATIVAMENTE INFORMACIÓN SOBRE LA SESIÓN)
806
LA RED DETERMINA EL IDENTIFICADOR ASOCIADO AL TERMINAL DE ACCESO (POR EJEMPLO, IDENTIFICADORES DE CSG)
808
LA RED DEVUELVE IDENTIFICADOR(ES)
810
EL PUNTO DE ACCESO RESTRINGIDO DETERMINA SI SE PERMITE EL ACCESO BASÁNDOSE EN EL (LOS) IDENTIFICADOR(ES)
812

FIG. 8

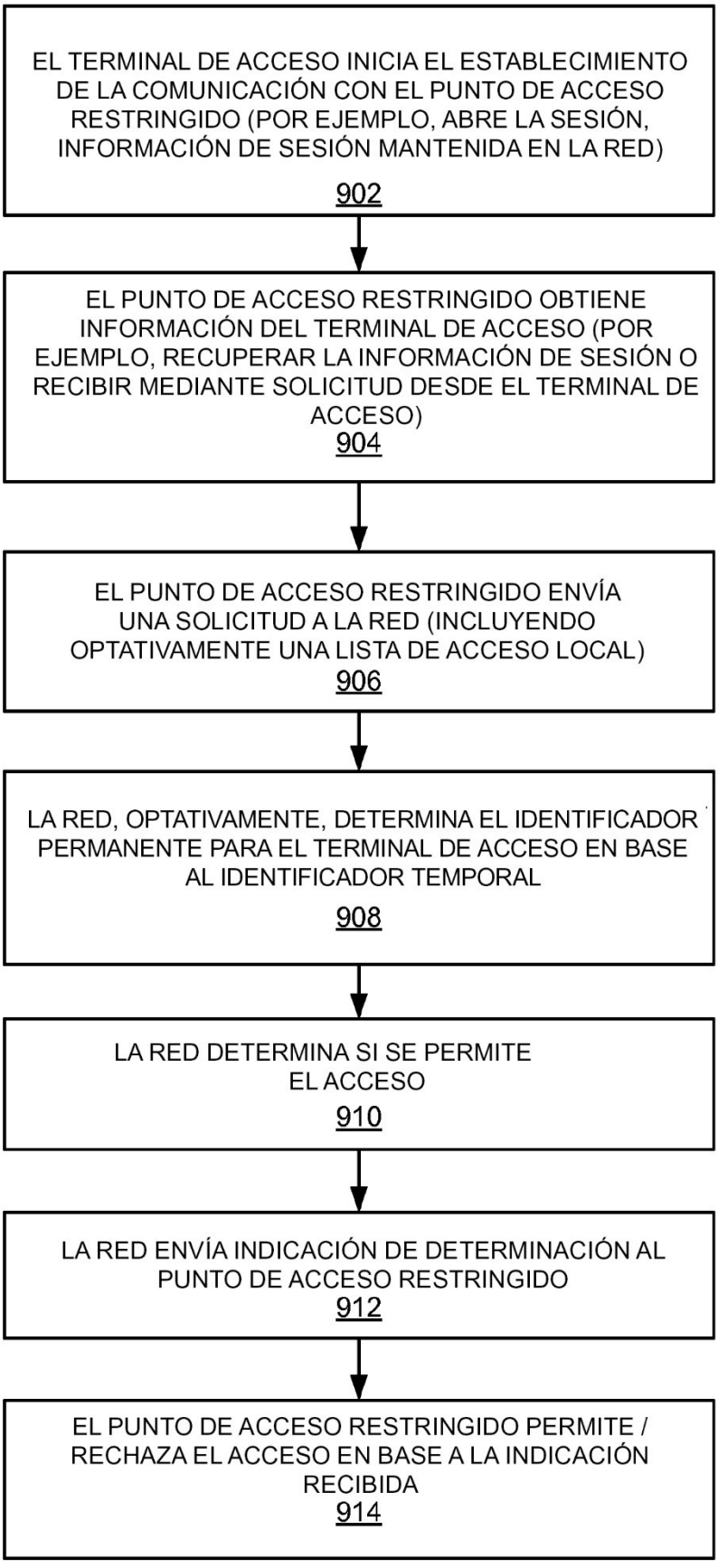
EL TERMINAL DE ACCESO INICIA EL ESTABLECIMIENTO DE LA COMUNICACIÓN CON EL PUNTO DE ACCESO RESTRINGIDO (POR EJEMPLO, ABRE LA SESIÓN, INFORMACIÓN DE SESIÓN MANTENIDA EN LA RED)
902
EL PUNTO DE ACCESO RESTRINGIDO OBTIENE INFORMACIÓN DEL TERMINAL DE ACCESO (POR EJEMPLO, RECUPERAR LA INFORMACIÓN DE SESIÓN O RECIBIR MEDIANTE SOLICITUD DESDE EL TERMINAL DE ACCESO)
904
EL PUNTO DE ACCESO RESTRINGIDO ENVÍA UNA SOLICITUD A LA RED (INCLUYENDO OPTATIVAMENTE UNA LISTA DE ACCESO LOCAL)
906
LA RED, OPTATIVAMENTE, DETERMINA EL IDENTIFICADOR PERMANENTE PARA EL TERMINAL DE ACCESO EN BASE AL IDENTIFICADOR TEMPORAL
908
LA RED DETERMINA SI SE PERMITE EL ACCESO
910
LA RED ENVÍA INDICACIÓN DE DETERMINACIÓN AL PUNTO DE ACCESO RESTRINGIDO
912
EL PUNTO DE ACCESO RESTRINGIDO PERMITE / RECHAZA EL ACCESO EN BASE A LA INDICACIÓN RECIBIDA
914

FIG. 9

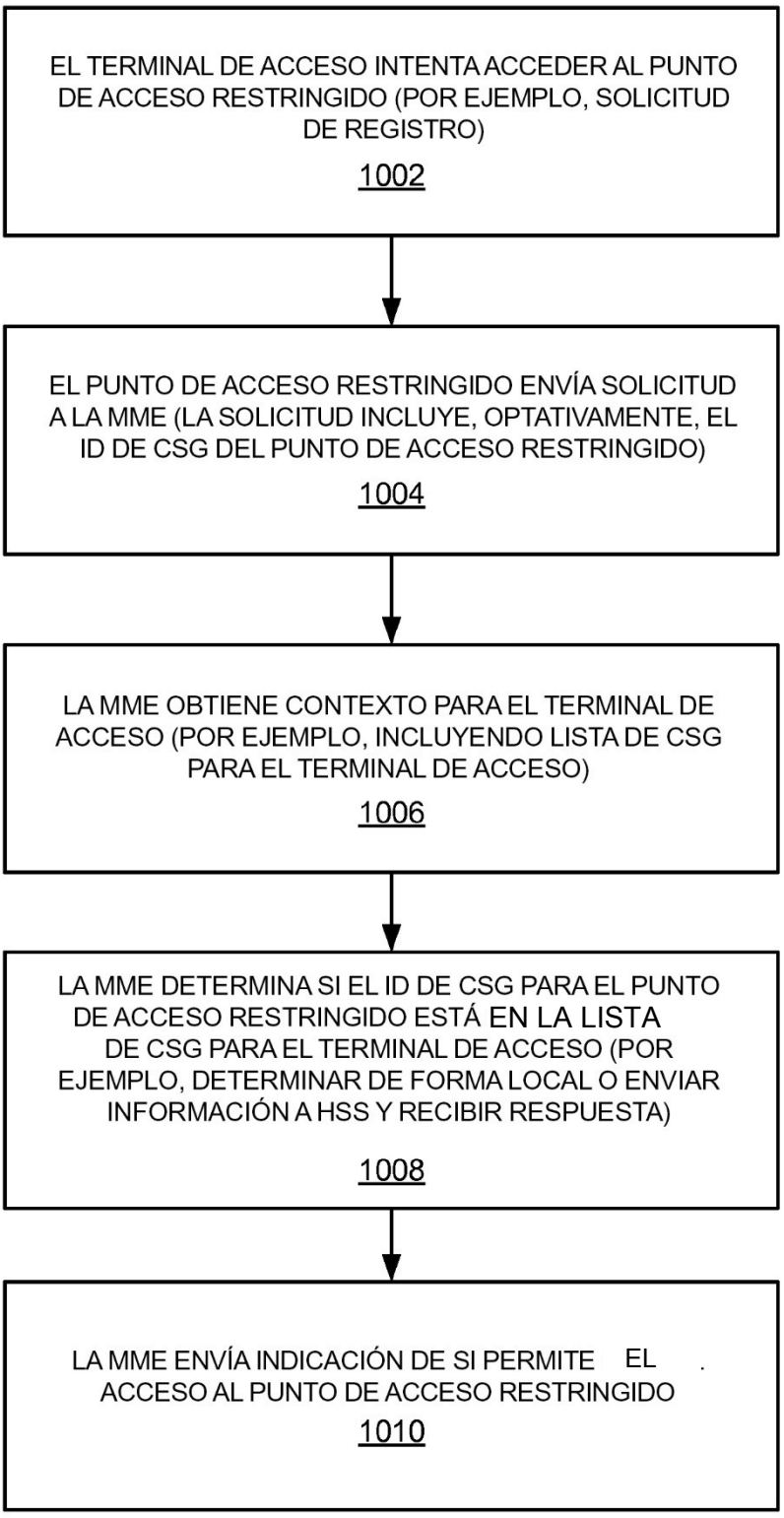
EL TERMINAL DE ACCESO INTENTA ACCEDER AL PUNTO DE ACCESO RESTRINGIDO (POR EJEMPLO, SOLICITUD DE REGISTRO)
1002
EL PUNTO DE ACCESO RESTRINGIDO ENVÍA SOLICITUD A LA MME (LA SOLICITUD INCLUYE, OPTATIVAMENTE, EL ID DE CSG DEL PUNTO DE ACCESO RESTRINGIDO)
1004
LA MME OBTIENE CONTEXTO PARA EL TERMINAL DE ACCESO (POR EJEMPLO, INCLUYENDO LISTA DE CSG PARA EL TERMINAL DE ACCESO)
1006
LA MME DETERMINA SI EL ID DE CSG PARA EL PUNTO DE ACCESO RESTRINGIDO ESTÁ EN LA LISTA DE CSG PARA EL TERMINAL DE ACCESO (POR EJEMPLO, DETERMINAR DE FORMA LOCAL O ENVIAR INFORMACIÓN A HSS Y RECIBIR RESPUESTA)
1008
LA MME ENVÍA INDICACIÓN DE SI PERMITE EL ACCESO AL PUNTO DE ACCESO RESTRINGIDO
1010

FIG. 10

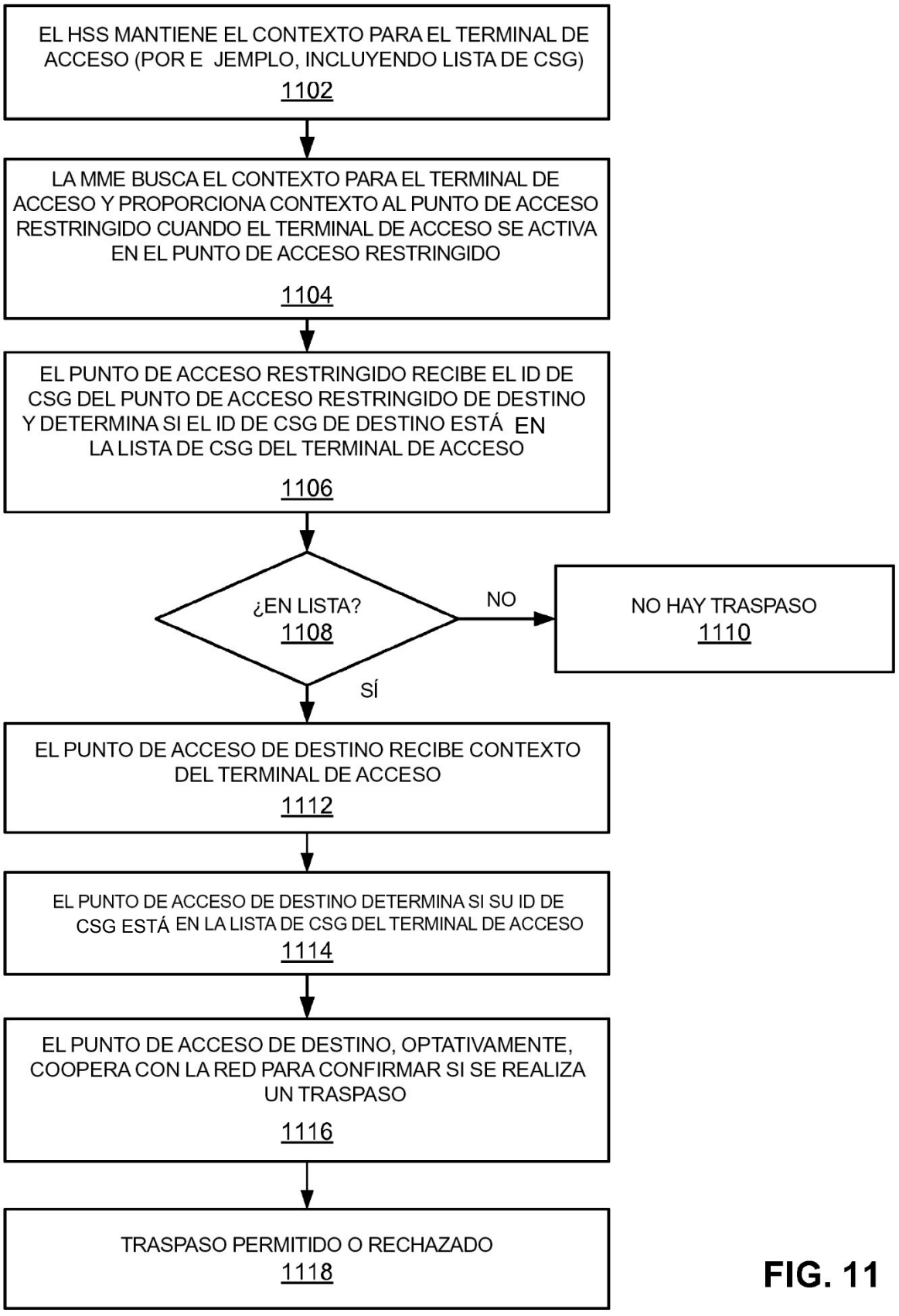
EL HSS MANTIENE EL CONTEXTO PARA EL TERMINAL DE ACCESO (POR E JEMPLO, INCLUYENDO LISTA DE CSG)
1102
LA MME BUSCA EL CONTEXTO PARA EL TERMINAL DE ACCESO Y PROPORCIONA CONTEXTO AL PUNTO DE ACCESO RESTRINGIDO CUANDO EL TERMINAL DE ACCESO SE ACTIVA EN EL PUNTO DE ACCESO RESTRINGIDO
1104
EL PUNTO DE ACCESO RESTRINGIDO RECIBE EL ID DE CSG DEL PUNTO DE ACCESO RESTRINGIDO DE DESTINO Y DETERMINA SI EL ID DE CSG DE DESTINO ESTÁ EN LA LISTA DE CSG DEL TERMINAL DE ACCESO
1106
¿EN LISTA?
1108
NO
NO HAY TRASPASO
1110
SÍ
EL PUNTO DE ACCESO DE DESTINO RECIBE CONTEXTO DEL TERMINAL DE ACCESO
1112
EL PUNTO DE ACCESO DE DESTINO DETERMINA SI SU ID DE CSG ESTÁ EN LA LISTA DE CSG DEL TERMINAL DE ACCESO
1114
EL PUNTO DE ACCESO DE DESTINO, OPTATIVAMENTE, COOPERA CON LA RED PARA CONFIRMAR SI SE REALIZA UN TRASPASO
1116
TRASPASO PERMITIDO O RECHAZADO
1118

FIG. 11

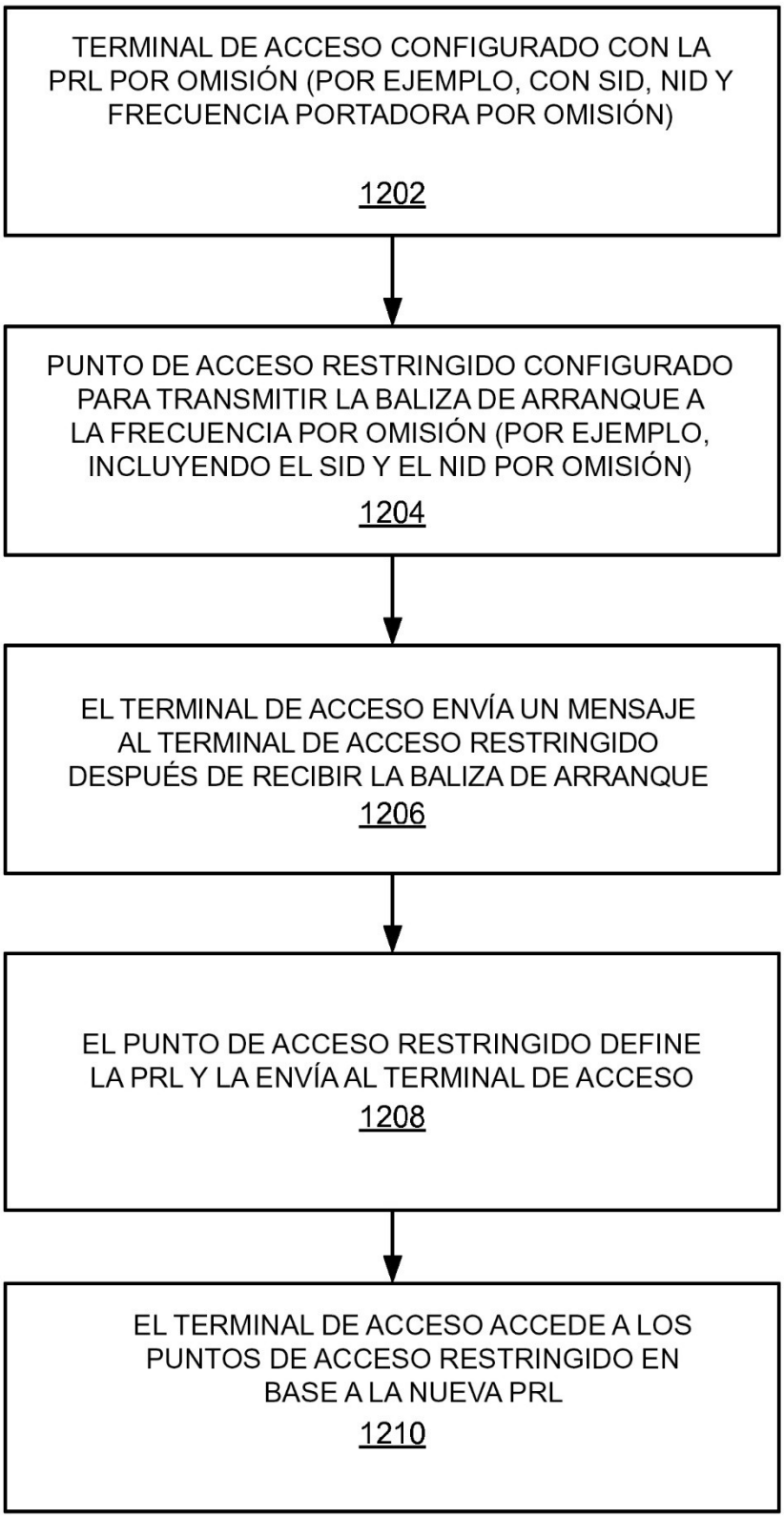
TERMINAL DE ACCESO CONFIGURADO CON LA PRL POR OMISIÓN (POR EJEMPLO, CON SID, NID Y FRECUENCIA PORTADORA POR OMISIÓN)
1202
PUNTO DE ACCESO RESTRINGIDO CONFIGURADO PARA TRANSMITIR LA BALIZA DE ARRANQUE A LA FRECUENCIA POR OMISIÓN (POR EJEMPLO, INCLUYENDO EL SID Y EL NID POR OMISIÓN)
1204
EL TERMINAL DE ACCESO ENVÍA UN MENSAJE AL TERMINAL DE ACCESO RESTRINGIDO DESPUÉS DE RECIBIR LA BALIZA DE ARRANQUE
1206
EL PUNTO DE ACCESO RESTRINGIDO DEFINE LA PRL Y LA ENVÍA AL TERMINAL DE ACCESO
1208
EL TERMINAL DE ACCESO ACCEDE A LOS PUNTOS DE ACCESO RESTRINGIDO EN BASE A LA NUEVA PRL
1210

FIG. 12

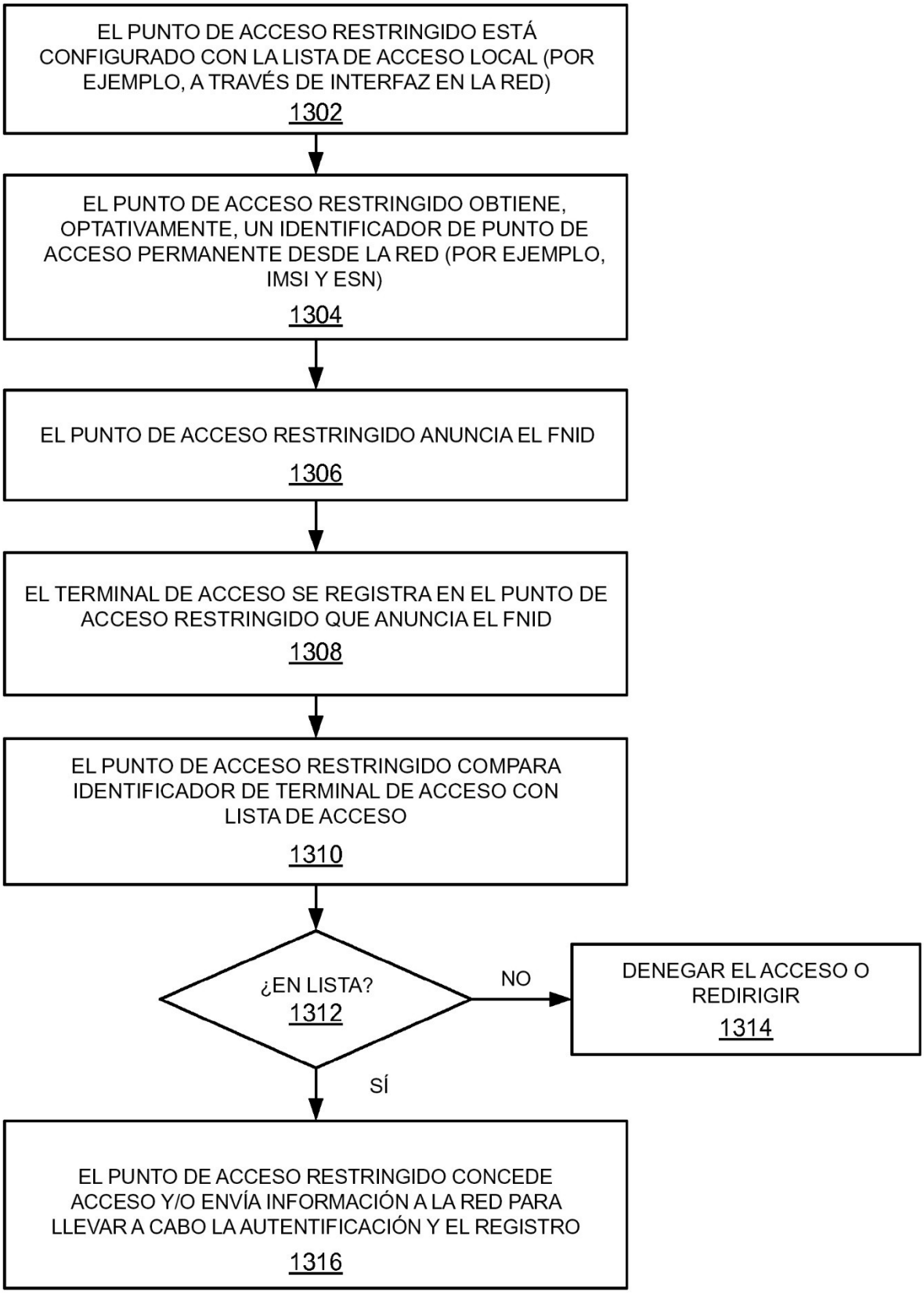
EL PUNTO DE ACCESO RESTRINGIDO ESTÁ CONFIGURADO CON LA LISTA DE ACCESO LOCAL (POR EJEMPLO, A TRAVÉS DE INTERFAZ EN LA RED)
1302
EL PUNTO DE ACCESO RESTRINGIDO OBTIENE, OPTATIVAMENTE, UN IDENTIFICADOR DE PUNTO DE ACCESO PERMANENTE DESDE LA RED (POR EJEMPLO, IMSI Y ESN)
1304
EL PUNTO DE ACCESO RESTRINGIDO ANUNCIA EL FNID
1306
EL TERMINAL DE ACCESO SE REGISTRA EN EL PUNTO DE ACCESO RESTRINGIDO QUE ANUNCIA EL FNID
1308
EL PUNTO DE ACCESO RESTRINGIDO COMPARA IDENTIFICADOR DE TERMINAL DE ACCESO CON LISTA DE ACCESO
1310
¿EN LISTA?
1312
NO
DENEGAR EL ACCESO O REDIRIGIR
1314
SÍ
EL PUNTO DE ACCESO RESTRINGIDO CONCEDE ACCESO Y/O ENVÍA INFORMACIÓN A LA RED PARA LLEVAR A CABO LA AUTENTIFICACIÓN Y EL REGISTRO
1316

FIG. 13

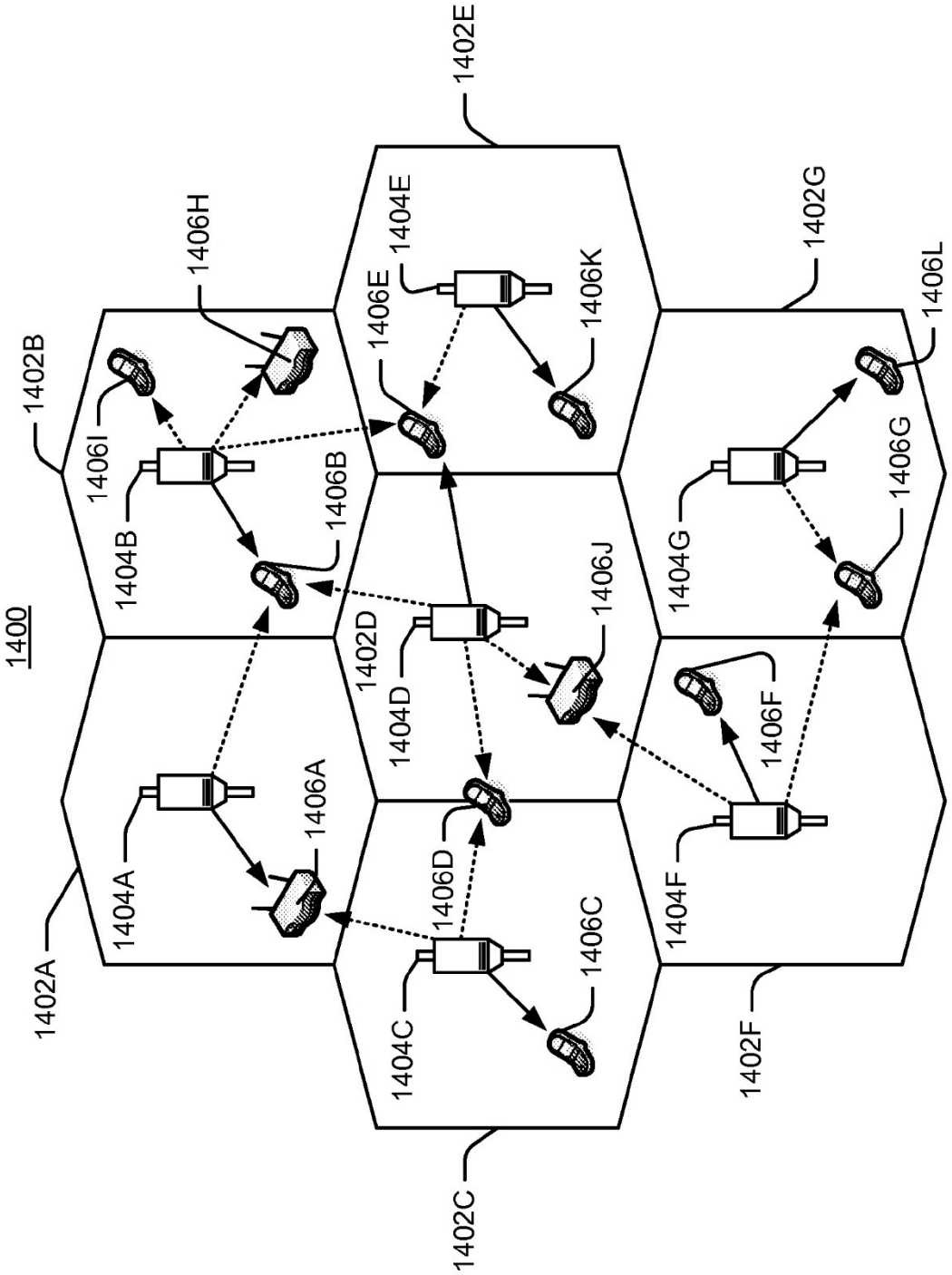
1400
1402A
1402B
1402C
1402D
1402E
1402F
1402G
1404A
1404B
1404C
1404D
1404E
1404F
1404G
1406A
1406B
1406C
1406D
1406E
1406F
1406G
1406H
1406I
1406J
1406K
1406L

FIG. 14

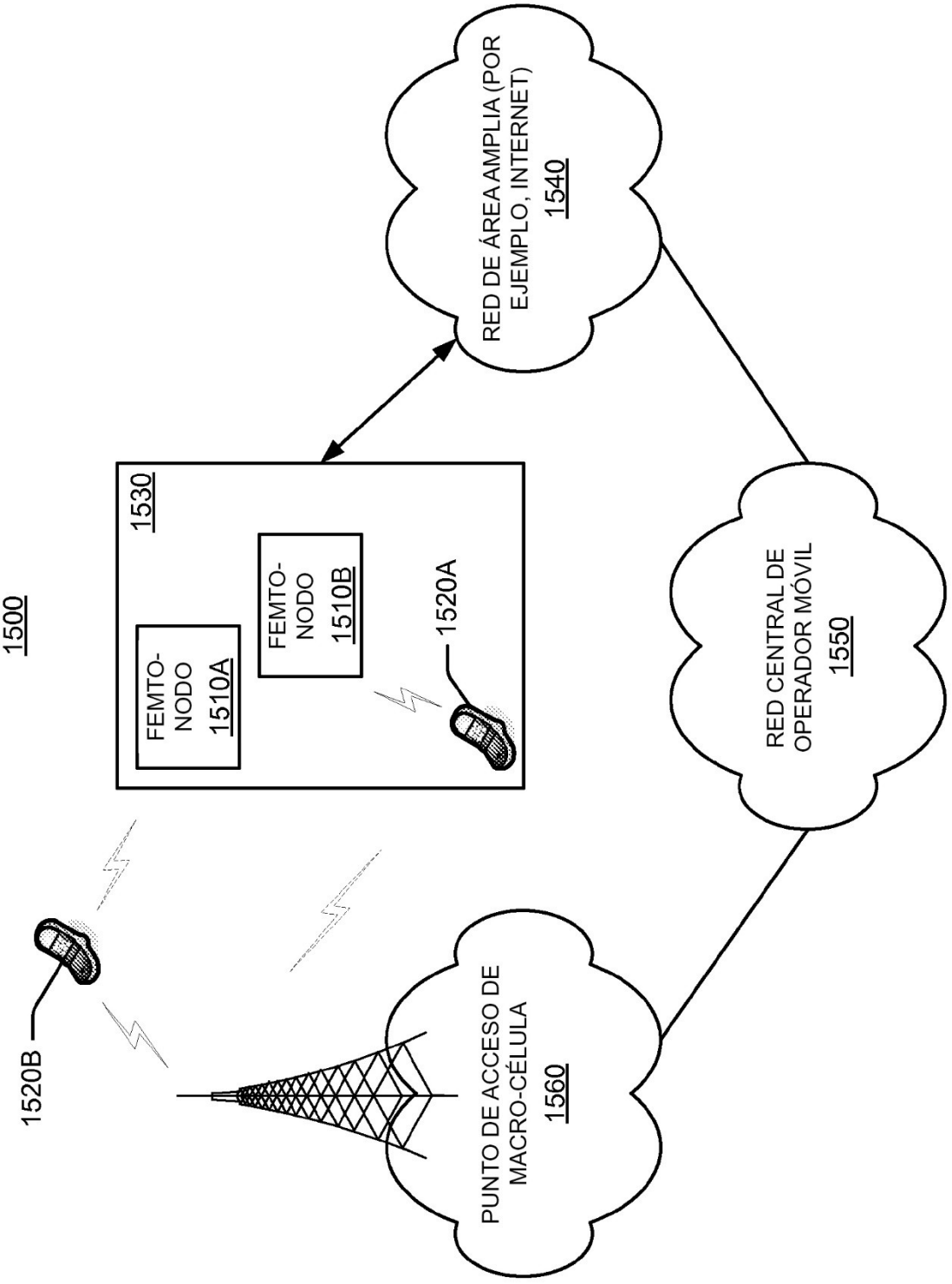
1500
1530
FEMTO-NODO 1510A
FEMTO-NODO 1510B
1520A
1520B
RED DE ÁREA AMPLIA (POR EJEMPLO, INTERNET) 1540
RED CENTRAL DE OPERADOR MÓVIL 1550
PUNTO DE ACCESO DE MACRO-CÉLULA 1560

FIG. 15

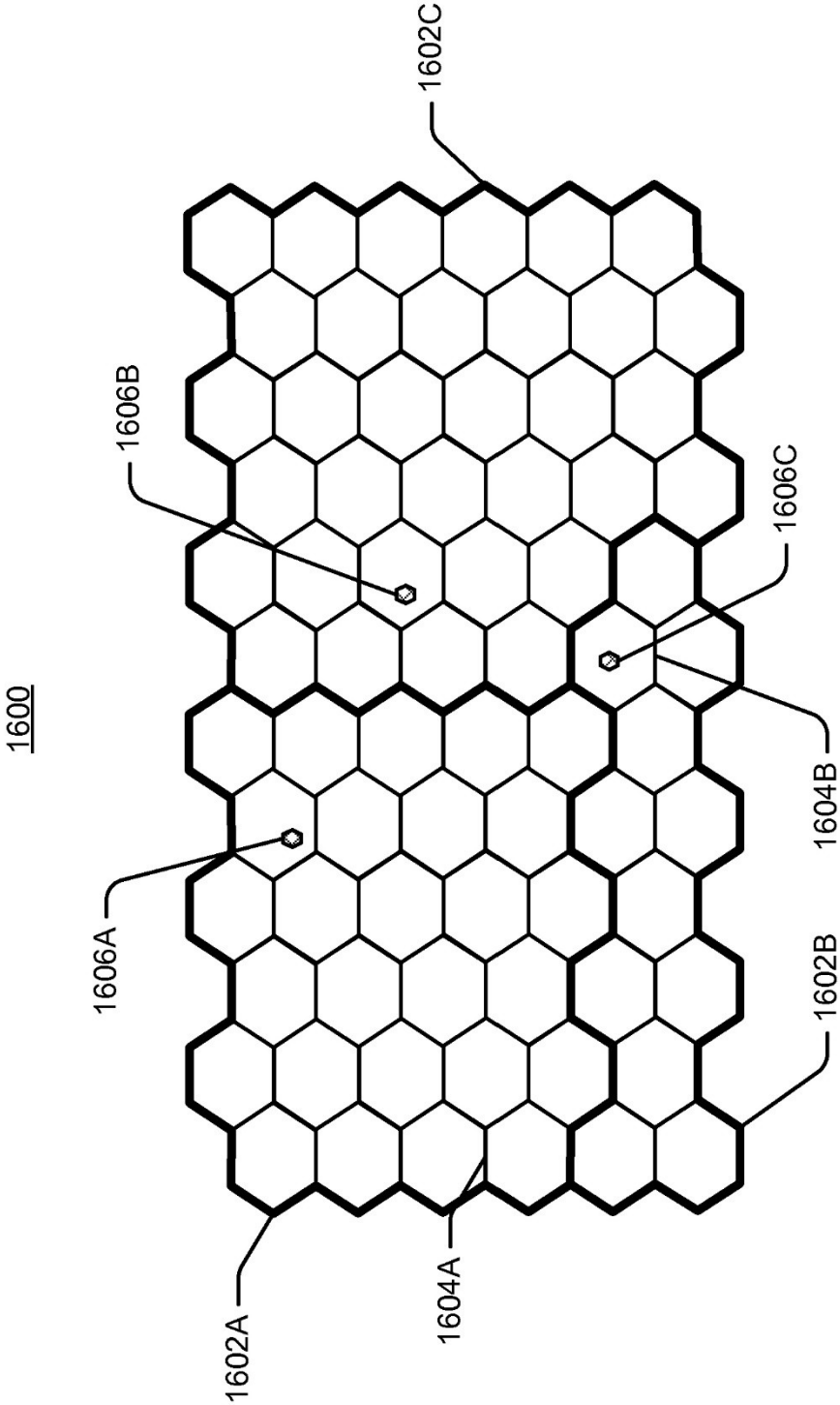

FIG. 16

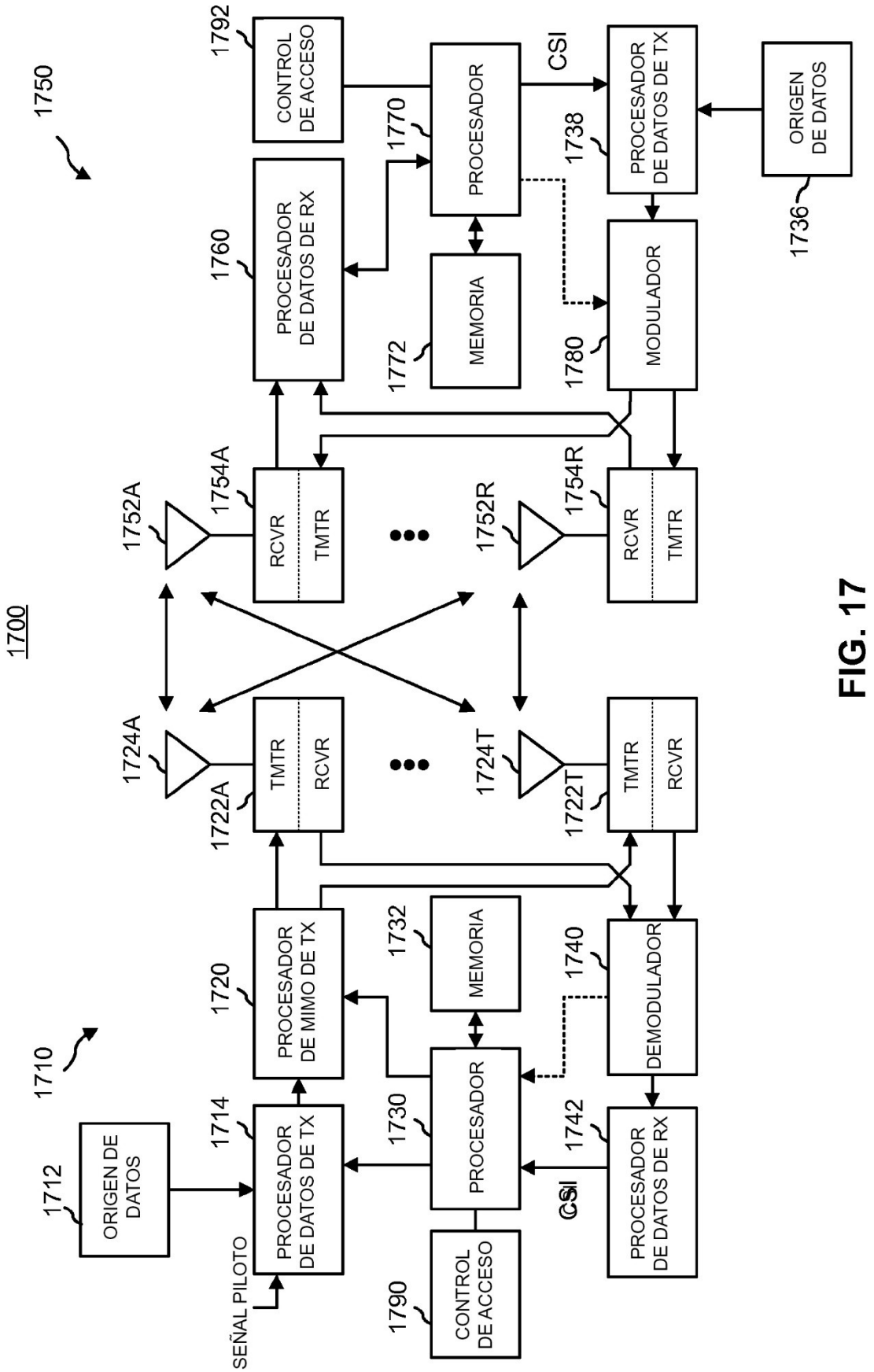
1700
1710
1712
ORIGEN DE DATOS
1714
PROCESADOR DE DATOS DE TX
SEÑAL PILOTO
1720
PROCESADOR DE MIMO DE TX
1722A
TMTR
RCVR
1724A
1724T
1722T
1730
PROCESADOR
1732
MEMORIA
1740
DEMODULADOR
1742
PROCESADOR DE DATOS DE RX
CSI
1790
CONTROL DE ACCESO
1750
1752A
1752R
1754A
1754R
RCVR
TMTR
1760
PROCESADOR DE DATOS DE RX
1770
PROCESADOR
1772
MEMORIA
1780
MODULADOR
1738
PROCESADOR DE DATOS DE TX
1736
ORIGEN DE DATOS
1792
CONTROL DE ACCESO
CSI

FIG. 17

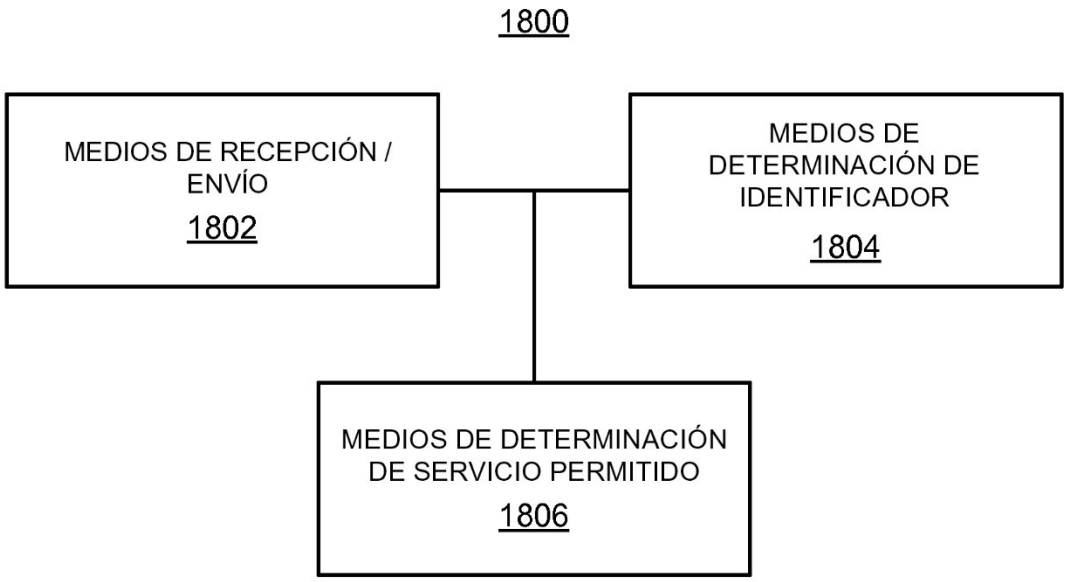
1800
MEDIOS DE RECEPCIÓN / ENVÍO
1802
MEDIOS DE DETERMINACIÓN DE IDENTIFICADOR
1804
MEDIOS DE DETERMINACIÓN DE SERVICIO PERMITIDO
1806

FIG. 18

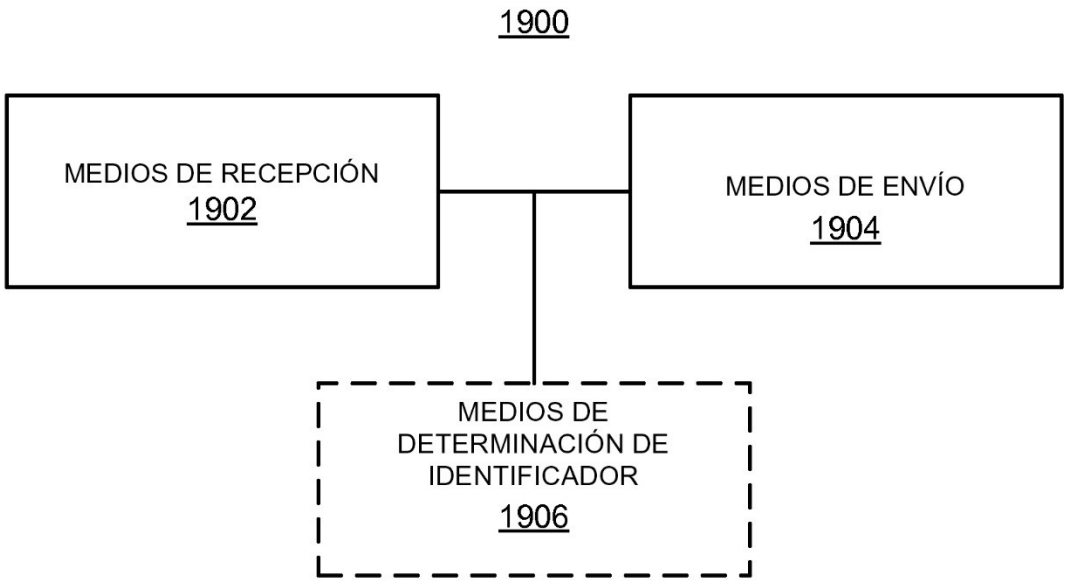
1900
MEDIOS DE RECEPCIÓN
1902
MEDIOS DE ENVÍO
1904
MEDIOS DE DETERMINACIÓN DE IDENTIFICADOR
1906

FIG. 19

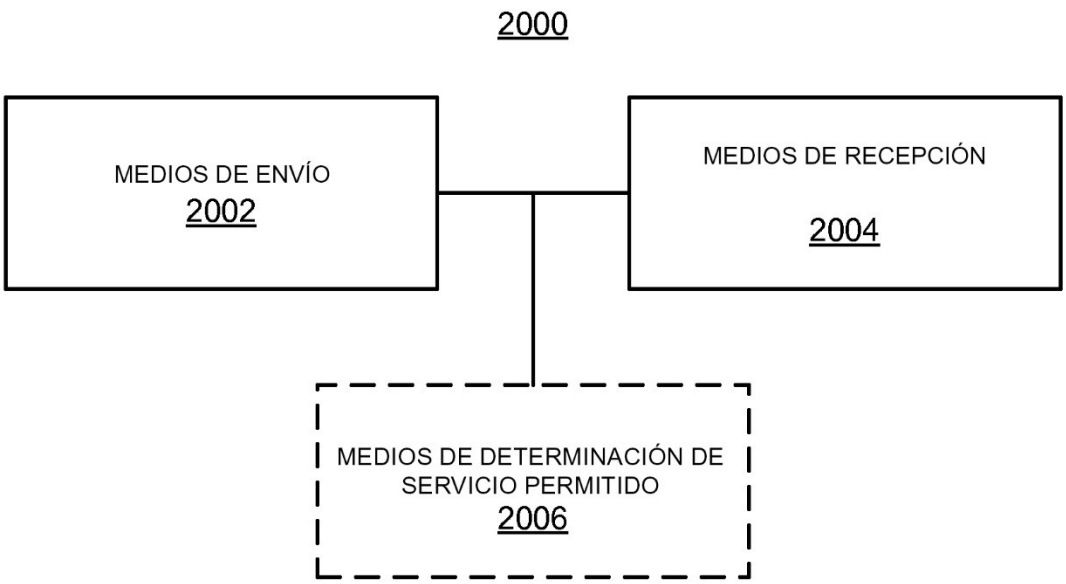
2000
MEDIOS DE ENVÍO
2002
MEDIOS DE RECEPCIÓN
2004
MEDIOS DE DETERMINACIÓN DE SERVICIO PERMITIDO
2006

FIG. 20

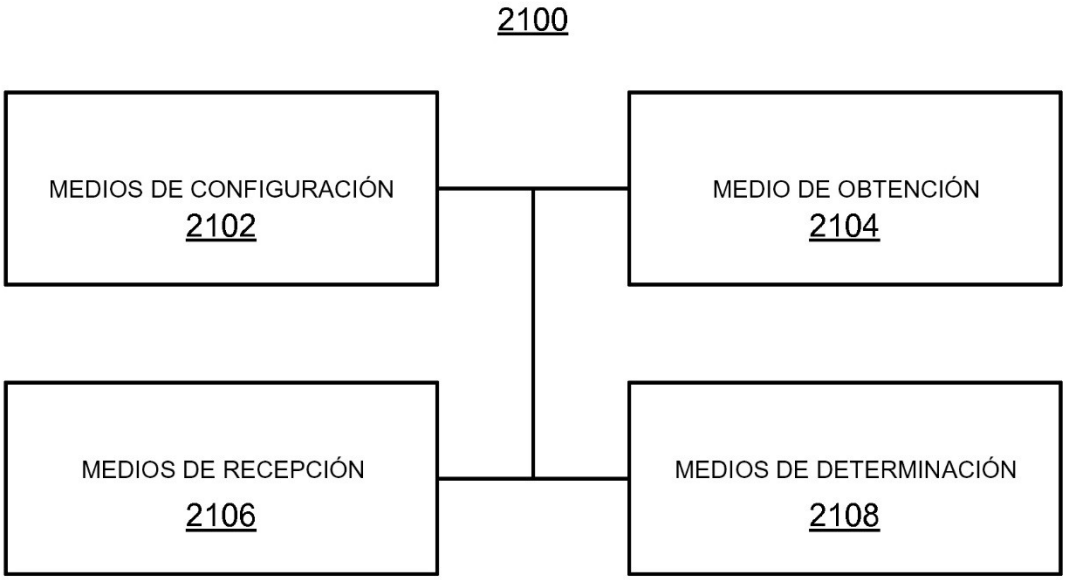
2100
MEDIOS DE CONFIGURACIÓN
2102
MEDIO DE OBTENCIÓN
2104
MEDIOS DE RECEPCIÓN
2106
MEDIOS DE DETERMINACIÓN
2108

FIG. 21

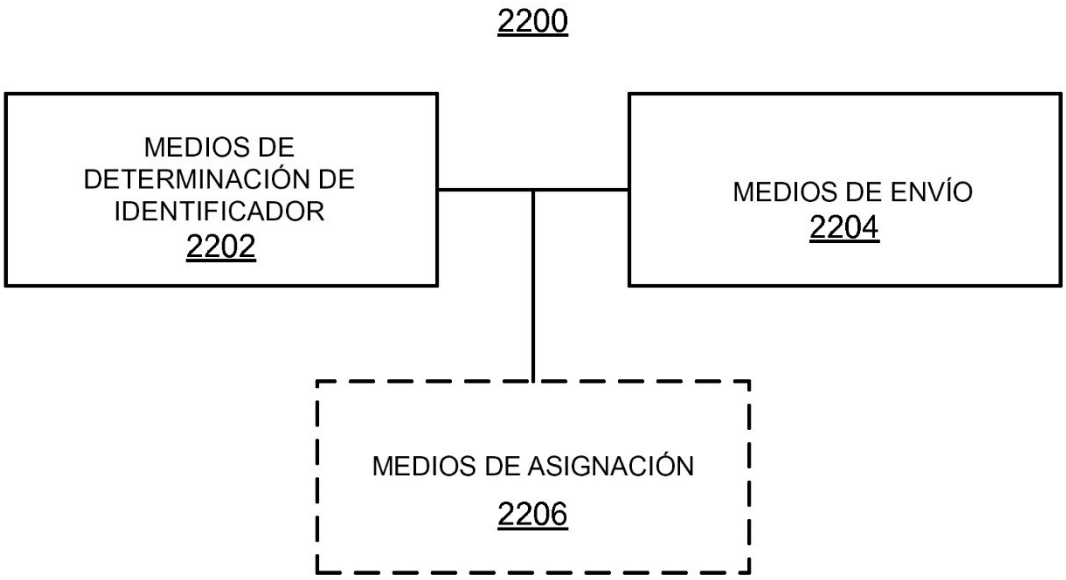

FIG. 22

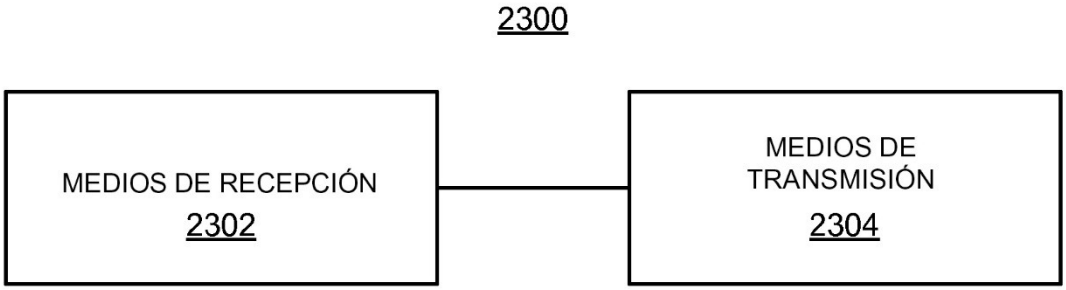

FIG. 23

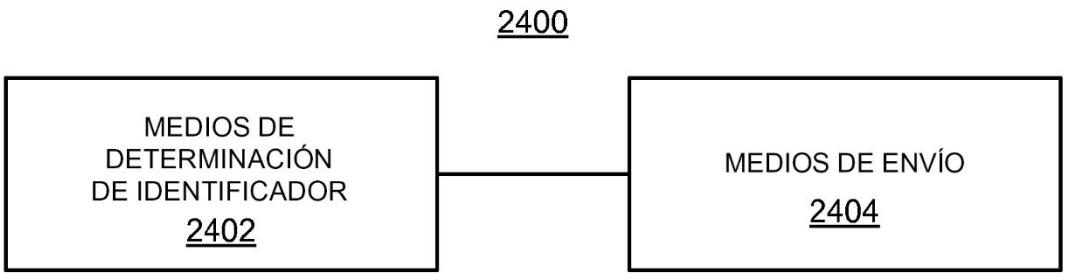

FIG. 24

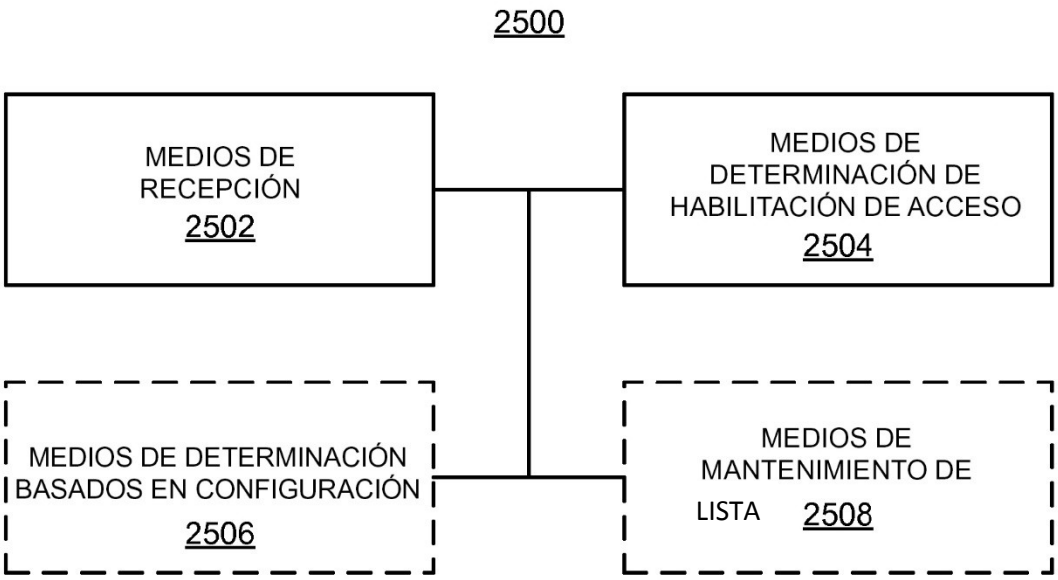
2500
MEDIOS DE RECEPCIÓN 2502
MEDIOS DE DETERMINACIÓN DE HABILITACIÓN DE ACCESO 2504
MEDIOS DE DETERMINACIÓN BASADOS EN CONFIGURACIÓN 2506
MEDIOS DE MANTENIMIENTO DE LISTA 2508

FIG. 25

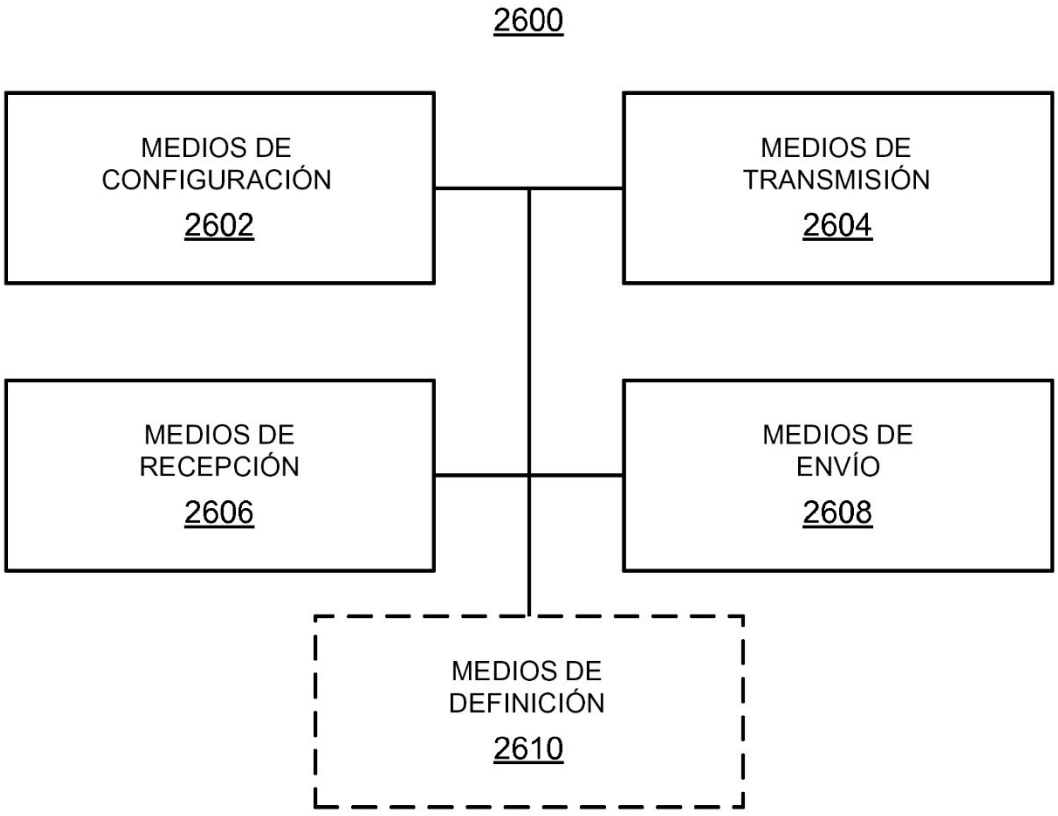
2600
MEDIOS DE CONFIGURACIÓN 2602
MEDIOS DE TRANSMISIÓN 2604
MEDIOS DE RECEPCIÓN 2606
MEDIOS DE ENVÍO 2608
MEDIOS DE DEFINICIÓN 2610

FIG. 26

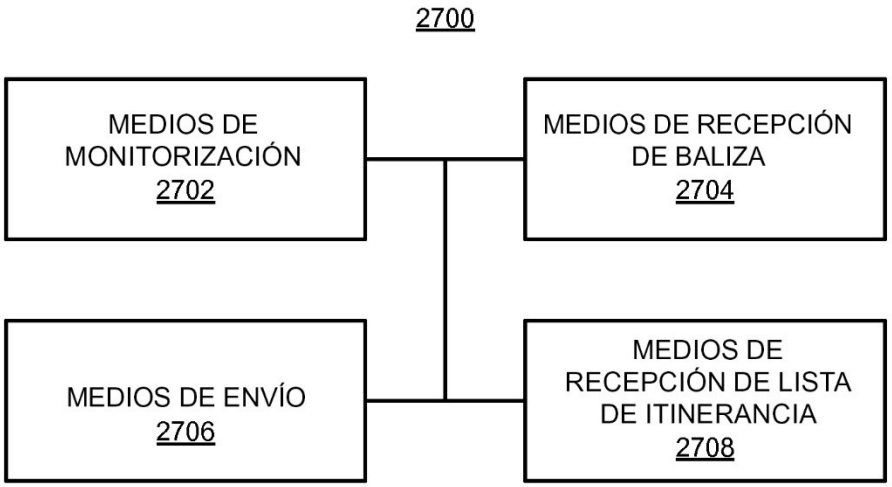
2700
MEDIOS DE MONITORIZACIÓN 2702
MEDIOS DE RECEPCIÓN DE BALIZA 2704
MEDIOS DE ENVÍO 2706
MEDIOS DE RECEPCIÓN DE LISTA DE ITINERANCIA 2708

FIG. 27

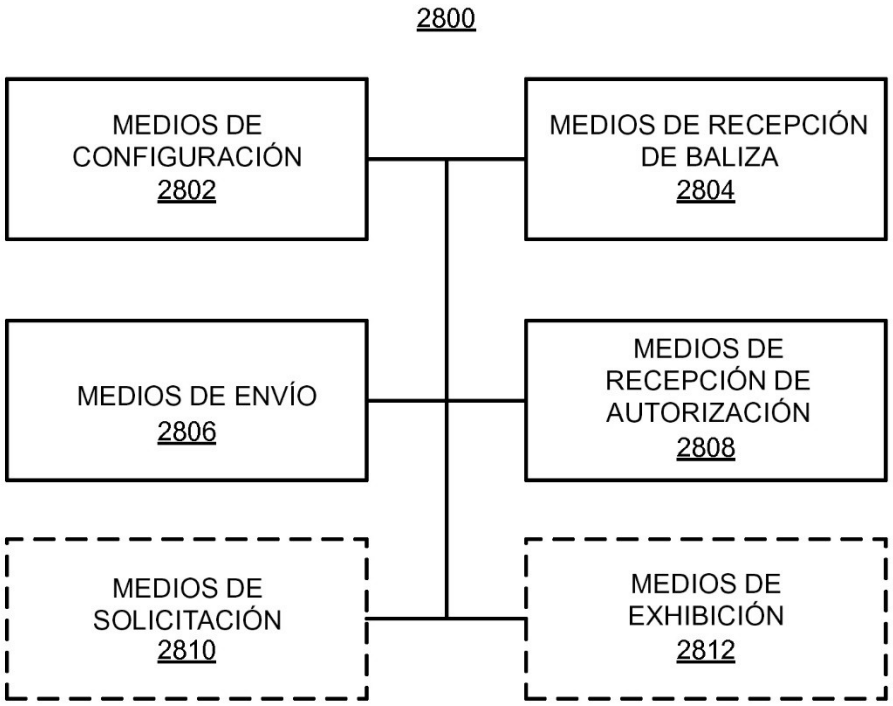
2800
MEDIOS DE CONFIGURACIÓN 2802
MEDIOS DE RECEPCIÓN DE BALIZA 2804
MEDIOS DE ENVÍO 2806
MEDIOS DE RECEPCIÓN DE AUTORIZACIÓN 2808
MEDIOS DE SOLICITACIÓN 2810
MEDIOS DE EXHIBICIÓN 2812

FIG. 28