

**PROHIBICIÓN DE ACCESO ESPECÍFICO DE SEGMENTO DE RED PARA  
REDES INALÁMBRICAS**

Campo técnico

5            Esta descripción se refiere a las comunicaciones.

Antecedentes

Un sistema de comunicación puede ser una instalación que posibilita la comunicación entre dos o más nodos o dispositivos, tales como dispositivos de comunicación fija o móvil. Las señales pueden llevarse en portadoras alámbricas  
10    o inalámbricas.

Un ejemplo de un sistema de comunicación celular es una arquitectura que se está normalizando por el Proyecto Común de Tecnologías Inalámbricas de la 3ª Generación (3GPP). Un desarrollo reciente en este campo a menudo se denomina como la evolución a largo plazo (LTE) de la tecnología de acceso por  
15    radio del Sistema Universal de Telecomunicaciones Móviles (UMTS). La E-UTRA (Acceso de Radio Terrestre de UMTS evolucionado) es la interfaz aérea de la ruta de mejora de la LTE del 3GPP para redes móviles. En LTE, las estaciones base o puntos de acceso (AP), que se denominan como AP de Nodo mejorado (eNB), proporcionan acceso inalámbrico dentro de un área de cobertura o célula.  
20    En LTE, los dispositivos móviles, o estaciones móviles se denominan como equipos de usuario (UE). LTE ha incluido un número de mejoras o desarrollos.

La escasez de ancho de banda global a la que se enfrentan las operadoras inalámbricas ha motivado la consideración del espectro de frecuencia de onda milimétrica (mmWave) infrautilizado para redes de  
25    comunicación celular de banda ancha futura, por ejemplo, de tipo mmWave (o

frecuencia extremadamente alta) puede incluir, por ejemplo, el intervalo de frecuencia entre 30 y 300 gigahercios (GHz). Las ondas de radio en esta banda pueden tener, por ejemplo, longitudes de onda de decenas a milímetros, lo que le proporciona el nombre de banda milimétrica de u onda milimétrica. La cantidad  
5 de datos inalámbricos aumentará probablemente de manera significativa en los próximos años. Se han usado diversas técnicas para intentar tratar este desafío que incluye obtener más espectro, que tiene tamaños de célula más pequeñas, y usar tecnologías mejoradas que posibilitan más bits/s/Hz. Un elemento que puede usarse para obtener más espectro es moverse a frecuencias más altas,  
10 por ejemplo, por encima de 6 GHz. Para sistemas inalámbricos de la quinta generación (5G), se ha propuesto una arquitectura de acceso para despliegue de equipo de radio celular que emplea espectro de radio de tipo mmWave. Pueden usarse también otros espectros de ejemplo, tal como espectro de radio de tipo cmWave (por ejemplo, 3-30 GHz).

15        Además, las redes inalámbricas de 5G pueden soportar segmentación de red, en donde una única red física puede segmentarse en múltiples redes virtuales. Cada segmento de red puede incluir un conjunto de funciones de red lógicas que pueden soportar los requisitos de un caso de uso particular.

#### Sumario

20        De acuerdo con una implementación de ejemplo, un método incluye: detectar, por un dispositivo de usuario, un segmento de red asociado con un intento de acceso por el dispositivo de usuario para acceder a una red inalámbrica; y, hacer, por el dispositivo de usuario, una decisión de prohibición para el intento de acceso basándose en el segmento de red asociado con el  
25 intento de acceso.

De acuerdo con una implementación de ejemplo, un aparato incluye al menos un procesador y al menos una memoria que incluye instrucciones informáticas que, cuando se ejecutan por el al menos un procesador, provocan al aparato: detectar, por un dispositivo de usuario, un segmento de red asociado con un intento de acceso por el dispositivo de usuario para acceder a una red inalámbrica; y, hacer, por el dispositivo de usuario, una decisión de prohibición para el intento de acceso basándose en el segmento de red asociado con el intento de acceso.

De acuerdo con una implementación de ejemplo, un producto de programa informático incluye un medio de almacenamiento legible por ordenador y que almacena código ejecutable que, cuando se ejecuta por al menos un aparato de procesamiento de datos, está configurado para provocar que el al menos un aparato de procesamiento de datos realice un método que incluye: detectar, por un dispositivo de usuario, un segmento de red asociado con un intento de acceso por el dispositivo de usuario para acceder a una red inalámbrica; y, hacer, por el dispositivo de usuario, una decisión de prohibición para el intento de acceso basándose en el segmento de red asociado con el intento de acceso.

De acuerdo con una implementación de ejemplo, un método incluye: recibir, por una estación base de una o más entidades de red principales en una red inalámbrica, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; determinar, por la estación base basándose en la información de carga específica de segmento de red recibida, una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso; y enviar, por la

estación base a un dispositivo de usuario, la configuración de prohibición para reducir una carga en la red inalámbrica.

De acuerdo con una implementación de ejemplo, un aparato incluye al menos un procesador y al menos una memoria que incluye instrucciones  
5 informáticas que, cuando se ejecutan por el al menos un procesador, provocan al aparato: recibir, por una estación base de una o más entidades de red principales en una red inalámbrica, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; determinar, por la estación base basándose en la información de carga  
10 específica de segmento de red recibida, una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso; y enviar, por la estación base a un dispositivo de usuario, la configuración de prohibición para reducir una carga en la red inalámbrica.

De acuerdo con una implementación de ejemplo, un producto de  
15 programa informático incluye un medio de almacenamiento legible por ordenador y que almacena código ejecutable que, cuando se ejecuta por al menos un aparato de procesamiento de datos, está configurado para provocar que el al menos un aparato de procesamiento de datos realice un método que incluye: recibir, por una estación base de una o más entidades de red principales en una  
20 red inalámbrica, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; determinar, por la estación base basándose en la información de carga específica de segmento de red recibida, una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso; y enviar, por la  
25 estación base a un dispositivo de usuario, la configuración de prohibición para

reducir una carga en la red inalámbrica.

De acuerdo con una implementación de ejemplo, un método incluye: determinar, por una entidad de red principal, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; y enviar, por la entidad de red principal a una estación base, la información de carga específica de segmento de red.

De acuerdo con una implementación de ejemplo, un aparato incluye al menos un procesador y al menos una memoria que incluye instrucciones informáticas que, cuando se ejecutan por el al menos un procesador, provocan al aparato: determinar, por una entidad de red principal, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; y enviar, por la entidad de red principal a una estación base, la información de carga específica de segmento de red.

De acuerdo con una implementación de ejemplo, un producto de programa informático incluye un medio de almacenamiento legible por ordenador y que almacena código ejecutable que, cuando se ejecuta por al menos un aparato de procesamiento de datos, está configurado para provocar que el al menos un aparato de procesamiento de datos realice un método que incluye: determinar, por una entidad de red principal, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; y enviar, por la entidad de red principal a una estación base, la información de carga específica de segmento de red.

Los detalles de uno o más ejemplos de implementaciones se exponen en los dibujos adjuntos y la descripción a continuación. Otras características serán evidentes a partir de la descripción y los dibujos, y de las reivindicaciones.

### Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques de una red inalámbrica de acuerdo con una implementación de ejemplo.

5 La Figura 2 es un diagrama que ilustra una técnica de prohibición de acceso específica de red de acuerdo con una implementación de ejemplo.

La Figura 3 es un diagrama de flujo que ilustra una operación de un dispositivo de usuario de acuerdo con una implementación de ejemplo.

La Figura 4 es un diagrama de flujo que ilustra una operación de una estación base de acuerdo con una implementación de ejemplo.

10 La Figura 5 es un diagrama de flujo que ilustra una operación de una entidad de red principal de acuerdo con una implementación de ejemplo.

La Figura 6 es un diagrama que ilustra una red de acuerdo con una implementación de ejemplo.

15 La Figura 7 es un diagrama que ilustra un procedimiento global para prohibición de acceso para los intentos de acceso provocados por una capa superior de acuerdo con una implementación de ejemplo.

La Figura 8 es un diagrama que ilustra un procedimiento global para prohibición de acceso para intentos de acceso activados por la capa de RRC de acuerdo con una implementación de ejemplo.

20 La Figura 9 es un diagrama que ilustra un procedimiento para que un nodo de RAN establezca la configuración de prohibición para que se difunda de acuerdo con una implementación de ejemplo.

La Figura 10 es un diagrama que ilustra una técnica de prohibición de acceso específica de red de acuerdo con otra implementación de ejemplo.

25 La Figura 11 es un diagrama de bloques de un nodo o estación

inalámbrica (por ejemplo, estación base/punto de acceso, nodo de retransmisión o estación móvil/dispositivo de usuario) de acuerdo con una implementación de ejemplo.

#### Descripción detallada

5           La Figura 1 es un diagrama de bloques de una red 130 inalámbrica de acuerdo con una implementación de ejemplo. En la red 130 inalámbrica de la Figura 1, los dispositivos 131, 132, 133 y 135 de usuario, que pueden denominarse también como estaciones móviles (MS) o equipo de usuario (UE), pueden conectarse (y en comunicación) con una estación base (BS) 134, que  
10 también puede denominarse como un punto de acceso (AP), un Nodo B mejorado (eNB) un gNB (que puede ser una estación base de 5G) o un nodo de red. Al menos parte de las funcionalidades de un punto de acceso (AP), estación base (BS) o (e)Nodo B (eNB) pueden llevarse a cabo también por cualquier nodo, servidor o anfitrión que puede acoplarse de manera operativa a un transceptor,  
15 tal como una cabecera de radio remota. La BS (o AP) 134 proporciona cobertura inalámbrica dentro de una célula 136, que incluye los dispositivos 131, 132, 133 y 135 de usuario. Aunque únicamente se muestran cuatro dispositivos de usuario como que están conectados o fijados a la BS 134, puede proporcionarse cualquier número de dispositivos de usuario. La BS 134 también está conectada  
20 a una red 150 principal mediante una interfaz 151. Esto es simplemente un ejemplo sencillo de una red inalámbrica, y pueden usarse otras.

Un dispositivo de usuario (terminal de usuario, equipo de usuario (UE)) puede hacer referencia a un dispositivo informático portátil que incluye dispositivos de comunicación móvil inalámbrica que operan con o sin un módulo  
25 de identificación de abonado (SIM), incluyendo, pero sin limitación, los siguientes

tipos de dispositivos: una estación móvil (MS), un teléfono móvil, un teléfono celular, un teléfono inteligente, un asistente digital personal (PDA), un microteléfono, un dispositivo que usa un módem inalámbrico (dispositivo de alarma o medición, etc.), un portátil y/u ordenador de pantalla táctil, una tableta, una tableta con funciones de teléfono, una consola de juegos, un portátil y un dispositivo multimedia, como ejemplos. Debería apreciarse que un dispositivo de usuario puede ser también un dispositivo únicamente de enlace ascendente casi exclusivo, de los cuales un ejemplo es una cámara o cámara de vídeo que carga imágenes o clips de vídeo a una red.

En LTE (como un ejemplo), la red principal puede denominarse como el Núcleo de Paquetes Evolucionado (EPC), que puede incluir una Entidad de Gestión de Movilidad (MME) que puede manejar o ayudar con movilidad/traspaso de dispositivos de usuario entre BS, una o más pasarelas que pueden reenviar datos y señales de control entre las BS y redes de datos de paquetes o la Internet, y otras funciones o bloques de control.

Las diversas implementaciones de ejemplo pueden aplicarse a una amplia diversidad de tecnologías inalámbricas, redes inalámbricas, tales como LTE, LTE-A, 5G (Nueva Radio, o NR), redes de banda cmWave, y/o mmWave, o cualquier otra red inalámbrica o caso de uso. Se proporcionan redes de banda LTE, 5G, cmWave y mmWave únicamente como ejemplos ilustrativos, y las diversas implementaciones de ejemplo pueden aplicarse a cualquier tecnología inalámbrica/red inalámbrica. Las diversas implementaciones de ejemplo pueden aplicarse también a diversas diferentes aplicaciones, servicios o casos de uso, tales como, por ejemplo, comunicaciones de baja latencia de ultra fiabilidad (URLLC), Internet de las Cosas (IoT), banda ancha móvil mejorada,

comunicaciones masivas de tipo máquina (MMTC), vehículo a vehículo (V2V), vehículo a dispositivo, etc. Cada uno de estos casos de uso, o tipos de UE, puede tener su propio conjunto de requisitos.

Además, las redes inalámbricas de 5G pueden soportar segmentación de red, en donde una única red física puede segmentarse en múltiples redes virtuales. Cada segmento de red puede incluir, por ejemplo, un conjunto de funciones de red lógicas que pueden soportar los requisitos de un caso de uso particular. La segmentación de red puede permitir tratamiento diferenciado dependiendo de los requisitos de diferentes UE o grupos de UE. Con la segmentación (segmentación de red), un operador puede crear redes para soluciones optimizadas basándose en diferentes requisitos de servicio, QoS (calidad de servicio), funcionalidad, rendimiento, etc. Por medio de ejemplo ilustrativo, un segmento de red puede incluir, por ejemplo, una porción de uno o más recursos de red en una o más entidades de red, tal como una porción de, por ejemplo, uno o más de recursos computacionales, recursos de memoria, recursos de hardware, software o recursos funcionales, y/u otros recursos de red en una BS y/o en una o más entidades de red principales, por ejemplo, que pueden soportar un grupo de UE o soportar un caso de uso particular.

De acuerdo con una implementación de ejemplo, un UE y/o grupo de UE, por ejemplo, con requisitos de QoS similares o que ejecutan la misma aplicación, proporcionan una característica o funcionalidad común, para un caso de uso particular u otro aspecto común, pueden soportar un segmento de red o pueden estar atribuidos o asignados a un segmento de red, por ejemplo, donde un identificador de segmento de red (o identificador de segmento) puede identificar el segmento de red. Sin embargo, diferentes UE (por ejemplo, diferente tipo de

UE) y/o cada diferente grupo de UE, que puede estar asignado a diferentes segmentos de red, pueden tener diferentes requisitos de servicio. De acuerdo con una implementación de ejemplo, diferentes UE y/o cada uno de múltiples grupos de UE pueden estar asignados a un segmento de red diferente.

- 5           Adicionalmente, un UE puede tener un número de diferentes aplicaciones y/o flujos de datos (por ejemplo, sesiones de unidad de datos de protocolo) que pueden generar y/o recibir tráfico o datos. Por lo tanto, un UE puede asignarse a múltiples segmentos de red, por ejemplo, basándose en diferentes tipos de tráfico que pueden transmitirse a o desde el UE, diferentes aplicaciones que se
- 10   ejecutan en un UE, o diferentes casos de uso que puede soportar el UE. Por lo tanto, un UE puede estar asignado o estar permitido a usar una pluralidad de segmentos de red.

De acuerdo con una implementación de ejemplo, un segmento puede identificarse por un identificador de segmento, que puede incluir uno o más de lo

15   siguiente: un tipo de segmento/servicio (SST); un tipo de segmento/servicio (SST) y diferenciador de segmento (SD); y una Información de Asistencia de Selección de Segmento de Red único (S-NSSAI). Por ejemplo un SST puede indicar un tipo de servicio, tal como un tipo de servicio inalámbrico de 5G específico, tal como comunicaciones de baja latencia de ultra fiabilidad,

20   (URLLC), Internet de las Cosas (IoT), banda ancha móvil mejorada (eMBB), comunicaciones masivas de tipo máquina (MMTC), etc. Por lo tanto, por ejemplo, un segmento de red puede estar asignado a o asociado con un tipo de servicio específico. Un diferenciador de segmento (SD) puede permitir adicionalmente una diferenciación entre diferentes segmentos del mismo tipo (por ejemplo, para

25   permitir la diferenciación entre dos segmentos de red de URLLC que pueden

asignarse a diferentes grupos de UE de URLLC, por ejemplo). También, de acuerdo con una implementación de ejemplo, una S-NSSAI puede ser otro tipo de identificador de segmento. De acuerdo con una implementación de ejemplo, una S-NSSAI = SST+SD (por ejemplo, S-NSSAI puede incluir o puede ser una combinación de o concatenación de un SST y un SD para un segmento), por ejemplo.

Como se indica, cada uno de los diferentes tipos de servicio inalámbricos (por ejemplo, URLLC, IoT, eMBB, mMTC) puede tener diferentes requisitos en términos de, por ejemplo, latencia, QoS, tasas de datos mínimas, etc. Como resultado, en algunos casos, diferentes tipos de servicios/servicio inalámbricos (por ejemplo, URLLC, IoT, eMBB, mMTC) pueden priorizarse para el servicio de manera diferente por una red inalámbrica. Puesto que cada segmento de red puede estar asociado con o asignado a un tipo de servicio inalámbrico específico (por ejemplo, URLLC, IoT, eMBB, mMTC), esto significa que, al menos en algunos casos, una red inalámbrica puede priorizar algunos segmentos de red sobre otros segmentos de res.

De acuerdo con una implementación de ejemplo, para obtener una conexión de radio, un dispositivo de usuario (UE) puede hacer principalmente un intento de acceso hacia la RAN (red de acceso de radio, que incluye una BS). En el caso donde una BS y/o red principal estén sobrecargadas (por ejemplo, demasiados UE que están usando y/o intentando usar recursos de red de la red y/o se está usando y/o se ha asignado un porcentaje umbral (por ejemplo, el 90 %+ ) de recursos de red), el intento de acceso por el UE puede prohibirse o evitarse por el UE. Si no se prohíbe el intento de acceso por el UE, entonces el UE puede enviar, por ejemplo, una solicitud de conexión de RRC (control de

recursos de radio) a una BS o entidad de red de acceso de radio, por ejemplo, para registrar y/o establecer una conexión (por ejemplo, conexión de RRC) a la red.

Por lo tanto, de acuerdo con una implementación de ejemplo, una red  
5 puede imponer restricciones de acceso a UE que están en un modo en espera (por ejemplo, modo RRC\_Idle), por ejemplo, para evitar que los UE se registren y/o establezcan una conexión de RRC a la red. Por ejemplo, una red inalámbrica puede difundir (por ejemplo, mediante información de sistema) una configuración de prohibición a uno o más UE. La configuración de prohibición puede indicar,  
10 por ejemplo, si se está realizando prohibición de acceso para una o más clases de acceso o categorías de acceso. Por ejemplo, a cada UE puede asignarse una clase de acceso. También, a cada intento de acceso puede asignarse una categoría de acceso. La red (por ejemplo, BS) puede difundir una configuración de prohibición a uno o más UE que puede incluir información que indica que los  
15 intentos de acceso asociados con una o más categorías de acceso y/o clases de acceso, por ejemplo, pueden prohibirse, y en caso afirmativo, proporcionar un conjunto de parámetros de prohibición para estas una o más clases y/o categorías de acceso, por ejemplo.

De acuerdo con una implementación de ejemplo, un conjunto de  
20 parámetros de prohibición puede incluir, por ejemplo, una tasa de prohibición (o factor de prohibición) y un tiempo de prohibición (o valor de temporizador de prohibición). Si se realiza prohibición de acceso (por ejemplo, para una clase de acceso o categoría de acceso), entonces el UE puede generar un número aleatorio. Si el número es, por ejemplo, menor que la tasa de prohibición  
25 (también conocido como el factor de prohibición), entonces no se prohíbe el

intento de acceso, y el UE puede acceder a la red enviando la solicitud de conexión de RRC. Si, por ejemplo, el número aleatorio generado por el UE es mayor o igual que la tasa de prohibición (o factor de prohibición), entonces se prohíbe el intento de acceso (al menos temporalmente), y no se permite que el

5 UE envíe la solicitud de conexión de RRC en ese momento, y el UE puede reintentar de nuevo más tarde el acceso de red después de que se haya agotado el temporizador de prohibición (por ejemplo, puede iniciarse el temporizador de prohibición y comenzar la cuenta atrás en o alrededor cuando se determina que el UE número aleatorio es mayor o igual que la tasa de prohibición, por ejemplo).

10 Por lo tanto, después del tiempo de prohibición, el UE puede de nuevo intentar acceder a la red, generando otro (un segundo) número aleatorio, y determinando si este segundo número aleatorio es menor que la tasa de prohibición o factor de prohibición. Por supuesto, la red puede ajustar una carga de red ajustando uno o más de los parámetros de prohibición. Por ejemplo, la red puede ajustar, por

15 ejemplo, aumentar o reducir, el número o porcentaje de UE que acceden satisfactoriamente a la red aumentando la tasa de prohibición/factor de prohibición o reduciendo la tasa de prohibición/factor de prohibición, por ejemplo. También, la carga de red puede ajustarse variando o ajustando el tiempo de prohibición (por ejemplo, un tiempo de prohibición aumentado puede reducir la

20 carga de red).

Sin embargo, la prohibición de acceso principalmente no tiene en cuenta diferentes cargas y/o prioridades que pueden aplicarse a o asociarse con diferentes segmentos de red (por ejemplo, asociarse con diferentes tipos de servicio). Diferentes segmentos de red (o tipos de segmento) pueden tener

25 diferentes cargas. Por ejemplo, un primer segmento de red asociado con o

asignado a los UE de URLLC puede tener una carga del 90 %, un segundo segmento de red asociado con UE de IoT puede tener una carga del 60 %. De acuerdo con una implementación de ejemplo, puede ser deseable permitir que la red reduzca la carga global en la red reduciendo la carga para los dos  
5 segmentos de red de manera diferente (por ejemplo, basándose en diferentes conjuntos de parámetros de prohibición). Por lo tanto, por ejemplo, la red puede establecer una tasa de prohibición para los UE de IoT (del segundo segmento de red) a una tasa de prohibición (o factor de prohibición) del 20 % (por ejemplo, para prohibir o evitar, de media, el 80 % de los intentos de acceso de los UE de  
10 IoT), y establecer una tasa de prohibición para los UE de URLLC (del primer segmento de red) al 70 % (por ejemplo, para prohibir o evitar, de media, únicamente el 30 % de los intentos de acceso de URLLC), por ejemplo, para priorizar intentos de acceso de URLLC sobre intentos de acceso de IoT, mientras se reduce la carga de red, por ejemplo.

15 Por lo tanto, de acuerdo con una implementación de ejemplo, puede realizarse prohibición de acceso específica de segmento de red. Por ejemplo, un UE puede tomar una decisión de prohibición para un intento de acceso basándose en un segmento de red asociado con el intento de acceso.

La Figura 2 es un diagrama que ilustra una técnica de prohibición de  
20 acceso específica de red de acuerdo con una implementación de ejemplo. En el UE 132, la BS 134 y una entidad 150 de red principal están en comunicación, como se muestra. En 210, el UE 132 detecta un segmento de red asociado con un intento de acceso por el UE. Como se indica, el UE puede estar asignado a o asociado con uno o más segmentos de red, por ejemplo, un segmento de red  
25 diferente para cada uno de múltiples servicios de 5G. El UE 132 puede detectar

para cuál segmento o segmentos, por ejemplo, para cuál aplicación o aplicaciones o tipo o tipos de servicio, está generando el intento de acceso para el UE, por ejemplo.

En 212, la entidad 150 de red principal puede enviar al UE 132 uno o más  
5 filtros de categoría de acceso que indican una categoría de acceso asociada con uno o más segmentos de red. Por ejemplo, los filtros de categoría de acceso pueden indicar: la categoría de acceso X para el segmento de red N.º 1 (URLLC); y la categoría de acceso Y para el segmento de red N.º 2 (IoT). Estos son simplemente un par de filtros de categoría de acceso de ejemplo ilustrativos, que  
10 permiten que el UE 132 determine una categoría de acceso para un intento de acceso basándose en el segmento asociado con el intento de acceso. Como se indica a continuación, diferentes categorías de acceso pueden tratarse de manera diferente para prohibición de acceso, por ejemplo, para priorizar intentos de acceso para ciertos segmentos a través de intentos de acceso para otros  
15 segmentos, por ejemplo. Por ejemplo, la categoría de acceso X (para el URLLC) puede priorizarse (por ejemplo, una cantidad reducida de prohibición para la categoría de acceso X) a través de la categoría de acceso Y (por ejemplo, una cantidad superior de prohibición de intentos de acceso para la categoría de acceso Y).

20 En 214, el UE 132 puede determinar una categoría de acceso para el intento de acceso basándose en el segmento para el intento de acceso y los filtros de categoría de acceso.

En 216, la entidad 150 de red principal puede determinar una carga o  
cargas de red específicas de segmento para cada uno del uno o más segmentos  
25 de red. La carga puede medirse o determinarse como, por ejemplo, el número

de UE, cantidad de tráfico, porcentaje o cantidad de recursos para el segmento de red que se usan o asignan, etc. Por lo tanto, la entidad 150 de red principal puede determinar de manera separada una carga para cada uno del uno o más segmentos de red.

5           En 218, la entidad 150 de red principal puede enviar a la BS 134 la información de carga específica de segmento para uno o más segmentos de red.

          En 220, la BS 134 puede determinar, basándose en la información de carga específica de segmento, una configuración de prohibición, por ejemplo, que puede indicar una o más categorías de acceso: si la categoría de acceso se  
10       somete a prohibición, y proporcionar un conjunto de parámetros de prohibición para la categoría de acceso (por ejemplo, una tasa de prohibición o factor de prohibición, y un tiempo de prohibición, como se ha descrito anteriormente). También, una configuración de prohibición puede incluir un factor de compensación para ajustar (por ejemplo, reducir) una prohibición de intentos de  
15       acceso de UE inactivos.

          De acuerdo con una implementación de ejemplo, un UE puede estar conectado (y activo); en espera (no conectado), o conectado (conectado a la entidad de red principal) pero inactivo (modo inactivo). En un ejemplo de modo inactivo, la red principal determina que el UE está conectado, y por lo tanto no  
20       realiza radiobúsqueda al UE inactivo, sino que en su lugar, simplemente envía cualesquiera datos de enlace descendente a la BS para su entrega al UE inactivo. La BS puede a continuación realizar radiobúsqueda al UE inactivo para provocar que el UE establezca una conexión (si no tiene prohibido el acceso) y reciba los datos de enlace descendente para el UE inactivo. De acuerdo con una  
25       implementación de ejemplo, puede usarse un factor de compensación para

ajustar una tasa de prohibición para los UE inactivos. Por ejemplo, el factor de compensación puede proporcionarse y usarse por el UE al tomar una decisión de prohibición que puede proporcionar menos intentos de acceso prohibidos para los UE de modo inactivo, en comparación con UE de modo en espera (por ejemplo, una tasa inferior de prohibición de intentos de acceso para los UE de modo inactivo, en comparación con una tasa superior de prohibición de intentos de acceso de UE de modo en espera, por ejemplo).

En 222, la configuración de prohibición puede enviarse desde la BS 134 al UE 132.

En 224, el UE 132 puede tomar una decisión de prohibición para el intento de acceso del UE basándose en el segmento de red asociado con el intento de acceso. Por ejemplo, el UE 132 puede tomar una decisión de prohibición basándose en la categoría de acceso para la categoría de acceso del UE (que está basada en el segmento para el intento de acceso) y la configuración de prohibición (por ejemplo, que puede indicar si se está realizando prohibición de acceso para tal categoría de acceso, y/o proporcionar un conjunto de parámetros de prohibición (por ejemplo, una tasa de prohibición o factor de prohibición y un tiempo de prohibición, y posiblemente un factor de compensación para que los UE de modo inactivo ajusten la toma de decisión de prohibición si el UE está un modo inactivo) para la categoría de acceso que puede proporcionar parámetros para que el UE tome la decisión de prohibición de acceso para el intento de acceso del UE.

Por ejemplo, el UE 132 puede generar un número aleatorio y compararlo a la tasa de prohibición o factor de prohibición recibido. Si el número aleatorio es menor que (o como alternativa, mayor que) la tasa de prohibición o factor de

prohibición, entonces no se prohíbe el intento de acceso. Si, por otra parte, el número aleatorio generado por el UE es mayor o igual que (o como alternativa, menor o igual que) la tasa de prohibición o factor de prohibición, entonces el intento de acceso del UE se prohíbe (al menos temporalmente) o se evita que  
5    tenga lugar.

En 226, si el intento de acceso del UE no se prohíbe, entonces el UE puede realizar el intento de acceso (para acceder a la red), por ejemplo, enviando un mensaje de solicitud de conexión de RRC a la BS 134. Si se prohíbe el intento de acceso, entonces el UE puede esperar una cantidad de tiempo basándose en  
10    el tiempo de prohibición (un tiempo de retroceso), y a continuación puede generar un segundo número aleatorio, y compararlo a la tasa de prohibición o factor de prohibición de nuevo, para determinar si el segundo intento de acceso también está prohibido. Este proceso puede continuar, por ejemplo, recibiendo el UE 132 de manera repetitiva una indicación de un intento de acceso de UE  
15    asociado con un segmento de red particular, y determinando a continuación (por ejemplo, basándose en el segmento asociado con el intento de acceso, y/o basándose en la configuración de prohibición específica de segmento y/o filtros de categoría de acceso específicos de segmento) si el intento de acceso está prohibido o no.

20    Ejemplo 1: la Figura 3 es un diagrama de flujo que ilustra una operación de un dispositivo de usuario de acuerdo con una implementación de ejemplo. La operación 310 incluye detectar, por un dispositivo de usuario, un segmento de red o una aplicación asociada con un intento de acceso por el dispositivo de usuario para acceder a una red inalámbrica. La operación 320 incluye  
25    determinar, por el dispositivo de usuario, una categoría de acceso basándose en

el segmento de red detectado o aplicación detectada. La operación 330 incluye tomar, por el dispositivo de usuario, una decisión de prohibición para el intento de acceso basándose en el segmento de red asociado con el intento de acceso.

Ejemplo 2: de acuerdo con una implementación de ejemplo del ejemplo 1, en donde la toma de una decisión de prohibición comprende: tomar, por el dispositivo de usuario basándose en el segmento de red asociado con el intento de acceso, una decisión de que el intento de acceso no está prohibido; y comprendiendo el método adicionalmente, por el dispositivo de usuario basándose en la decisión, el intento de acceso detectado a la red inalámbrica.

Ejemplo 3: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-2, en donde la realización del intento de acceso detectado comprende: enviar, por el dispositivo de usuario, un mensaje de solicitud de conexión de control de recursos de radio (RRC) para solicitar una conexión a la red inalámbrica.

Ejemplo 4: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-3, y que comprende adicionalmente: recibir, por el dispositivo de usuario, uno o más filtros de categoría de acceso que indican una categoría de acceso asociada con uno o más segmentos de red o aplicaciones; determinar, por el dispositivo de usuario, una categoría de acceso para el intento de acceso basándose en el segmento de red o aplicación que está asociada con el intento de acceso y el uno o más filtros de categoría de acceso; recibir, por el dispositivo de usuario, una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso; y en donde la toma de una decisión de prohibición comprende tomar, por el dispositivo de usuario, una decisión de prohibición para el intento de acceso basándose en

la configuración de prohibición y la categoría de acceso para el intento de acceso.

Ejemplo 5: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-4, en donde el segmento de red asociado con el intento de acceso comprende uno o más de lo siguiente: un tipo de segmento/servicio (SST); un tipo de segmento/servicio (SST) y diferenciador de segmento (SD); una Información de Asistencia de Selección de Segmento de Red único (S-NSSAI).

Ejemplo 6: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-5, en donde la configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso comprende una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso y una o más aplicaciones.

Ejemplo 7: el método de cualquiera de las reivindicaciones 1-6 en donde la aplicación asociada con el intento de acceso se identifica por uno o más de lo siguiente: identidad de sistema operativo; e identidad de aplicación de sistema operativo.

Ejemplo 8: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-7, en donde la configuración de prohibición indica un conjunto de parámetros de prohibición, que incluye al menos una tasa de prohibición y un temporizador de prohibición, para una o más de las categorías de acceso.

Ejemplo 9: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-8, y que comprende adicionalmente: recibir un parámetro de compensación para un dispositivo de usuario en modo inactivo; determinar, por

el dispositivo de usuario, que el dispositivo de usuario está en modo inactivo; y en donde la toma de una decisión de prohibición comprende: aplicar, por el dispositivo de usuario, el parámetro de compensación a la toma de una decisión de prohibición para que el dispositivo de usuario ajuste una tasa de prohibición del intento de acceso del dispositivo de usuario que está en modo inactivo.

Ejemplo 10: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-9, en donde la configuración de prohibición está basada en una información de carga específica de segmento de red que indica una carga de red para cada uno del uno o más segmentos de red.

Ejemplo 11: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 1-10, en donde la configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso proporciona o indica una priorización diferente de uno o más intentos de acceso basándose en categorías de acceso de los intentos de acceso.

Ejemplo 12: la Figura 4 es un diagrama de flujo que ilustra una operación de una estación base de acuerdo con una implementación de ejemplo. La operación 410 incluye recibir, por una estación base de una o más entidades de red principales en una red inalámbrica, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red. La operación 420 incluye determinar, por la estación base basándose en la información de carga específica de segmento de red recibida, una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso. La operación 430 incluye enviar, por la estación base a un dispositivo de usuario, la configuración de prohibición para reducir una carga en la red inalámbrica.

Ejemplo 13: de acuerdo con una implementación de ejemplo del ejemplo 12, en donde el envío comprende enviar, por la estación base a un dispositivo de usuario, la configuración de prohibición, para permitir que el dispositivo de usuario tome una decisión de prohibición para un intento de acceso basándose en un segmento de red asociado con el intento de acceso por el dispositivo de usuario.

Ejemplo 14: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 12-13, y que comprende adicionalmente: reenviar, por la estación base al dispositivo de usuario, uno o más filtros de acceso que indican una categoría de acceso asociada con uno o más segmentos de red.

Ejemplo 15: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 12-14, en donde la configuración de prohibición indica un conjunto de parámetros de prohibición, que incluye al menos una tasa de prohibición y un temporizador de prohibición, para una o más de las categorías de acceso.

Ejemplo 16: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 12-15, en donde el uno o más segmentos de red se identifican por o están asociados con uno o más de lo siguiente: un tipo de segmento/servicio (SST); un tipo de segmento/servicio (SST) y diferenciador de segmento (SD); y una Información de Asistencia de Selección de Segmento de Red único (S-NSSAI).

Ejemplo 17: la Figura 5 es un diagrama de flujo que ilustra una operación de una entidad de red principal de acuerdo con una implementación de ejemplo. La operación 510 incluye determinar, por una entidad de red principal, información de carga específica de segmento de red que indica una carga para

cada uno del uno o más segmentos de red. La operación 520 incluye enviar, por la entidad de red principal a una estación base, la información de carga específica de segmento de red.

Ejemplo 18: de acuerdo con una implementación de ejemplo del ejemplo 5 17, en donde la entidad de red principal comprende una primera entidad de red principal, y en donde la información de carga específica de segmento de red se determina por la primera entidad de red principal de uno o más de lo siguiente: información de carga específica de segmento de red determinada o recogida por la primera entidad de red principal; e información de carga específica de 10 segmento de red recibida de una segunda entidad de red principal.

Ejemplo 19: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 17-18, y que comprende adicionalmente: enviar, por la entidad de red principal a un dispositivo de usuario mediante una estación base, uno o más filtros de categoría de acceso que indican una categoría de acceso asociada 15 con uno o más segmentos de red.

Ejemplo 20: de acuerdo con una implementación de ejemplo de cualquiera de los ejemplos 17-19, en donde el uno o más segmentos de red se identifican por o están asociados con uno o más de lo siguiente: un tipo de segmento/servicio (SST); un tipo de segmento/servicio (SST) y diferenciador de 20 segmento (SD); y una Información de Asistencia de Selección de Segmento de Red único (S-NSSAI).

Ejemplo 21: un aparato que comprende medios para realizar un método de cualquiera de los ejemplos 1-20.

Ejemplo 22: un aparato que comprende al menos un procesador y al 25 menos una memoria que incluye instrucciones informáticas que, cuando se

ejecutan por el al menos un procesador, provocan que el aparato realice un método de cualquiera de los ejemplos 1-20.

Ejemplo 23: un aparato que comprende un producto de programa informático que incluye un medio de almacenamiento legible por ordenador no transitorio y que almacena código ejecutable que, cuando se ejecuta por al menos un aparato de procesamiento de datos, está configurado para provocar que el al menos un aparato de procesamiento de datos realice un método de cualquiera de los ejemplos 1-20.

Se proporcionarán ahora implementaciones de ejemplo y/o detalles de ejemplo adicionales.

La Figura 6 es un diagrama que ilustra una red de acuerdo con una implementación de ejemplo. La figura anterior muestra una parte de la arquitectura 5GS en la representación del punto de referencia. El UE es servido por un nodo de RAN (BS) en RAN y por una AMF y una SMF en la red principal. Una vez que se registra el UE en la red, el UE puede comunicarse con una DN mediante una sesión de PDU: se establece una ruta de datos a través de RAN y UPF hacia una DN. Un registro del UE, movilidad, y sesiones se gestionan por las funciones de red del plano de control de la red principal: AMF y SMF. Además, se almacena una suscripción del UE en la política del UDM y el UE (por ejemplo, restricción de movilidad) se controla por la PCF.

Cuando es probable que se dé servicio al UE por la red, el UE necesita obtener la conexión de radio y registrarse en la red principal. Para obtener la conexión de radio, el UE hace un intento de acceso hacia la RAN (pero en primer lugar el UE debe confirmar que el intento de acceso no está prohibido. En caso de que la RAN y/o la red principal estén sobrecargadas, el intento de acceso

puede prohibirse por el UE. En una implementación de ejemplo, el UE puede prohibir un intento de acceso de acuerdo con las características del intento de acceso y la configuración de prohibición difundida por el nodo de RAN, y posiblemente otra información. Sin embargo, una prohibición de acceso  
5 tradicional no tiene en cuenta segmentos, información relacionada con el segmento o información de carga específica de segmento.

Por lo tanto, de acuerdo con una implementación de ejemplo, puede realizarse prohibición de acceso específica de segmento de red. Por ejemplo, un UE puede tomar una decisión de prohibición para un intento de acceso  
10 basándose en un segmento de red asociado con el intento de acceso.

De acuerdo con una implementación de ejemplo, puede enviarse un informe de carga desde la red principal (por ejemplo, AMF y/o SMF) a RAN/BS; prohibir la configuración para los UE de RRC inactivo (y conectado) a diferencia de los UE conectados y activos, y en espera; los UE de modo conectado no se  
15 prohíben normalmente; los UE de modo en espera no deberían prohibirse en su mayoría, y los UE conectados inactivos deberían prohibirse menos que los UE de modo en espera, puesto que la CN cree que estos UE están conectados. Por lo que estos UE inactivos reciben algunos parámetros de configuración de prohibición de acceso adicionales (por ejemplo, el parámetro de compensación).  
20 Una configuración de prohibición puede determinarse por la BS basándose en información de carga y enviarse al UE.

Una entidad de 5GMM del UE puede recopilar una o más de la siguiente información de otras entidades en el UE:  
el inicio y detención del vídeo de MMTel, voz de MMTel, servicios de SMSoIP de  
25 la entidad de IMS; solicitud de entrega de SMSoNAS de la entidad de SMS; e

indicación de si la solicitud de 5GSM está relacionada con la sesión de PDU de emergencia de la entidad de 5GSM. A continuación, el 5GMM de la entidad de UE decide la categoría de acceso de unos intentos de acceso haciendo uso de información disponible para sí misma además de la información anterior y envía  
5 la categoría de acceso a la capa de RRC del UE.

La capa de RRC toma una decisión de prohibición para el intento de acceso teniendo en cuenta los siguientes factores:

la configuración de prohibición es específica de categoría de acceso, que es específica de segmento (esta configuración de prohibición tiene en cuenta la  
10 información de carga específica de segmento; y, la transmisión de configuración de prohibición puede activarse por información de carga actualizada), categoría de acceso de la entidad de 5GMM;  
clase o clases de acceso del UE; y/o  
si el intento de acceso está activando el cambio de RRC-INACTIVO a RRC-  
15 CONECTADO y, en caso afirmativo, si el intento de acceso se activa por radiobúsqueda de nivel de RAN.

El UE decide si el intento de acceso está prohibido o no prohibido basándose en información que proviene de la BS - si está prohibido, a continuación el UE pasa en el modo en espera, y si no está prohibido, a  
20 continuación el UE pasa de RRC inactivo a RRC conectado; en RRC, hay tres estados diferentes - conectado, inactivo y en espera (en nivel de RRC).

El segmento (por ejemplo, SST) puede tenerse en cuenta para la decisión de categoría de acceso: la entidad de 5GMM recopila información de otras entidades, y la entidad de 5GMM puede recopilar con qué segmento (por  
25 ejemplo, SST) de la solicitud de acceso de 5GSM está relacionado desde la

entidad de 5GSM. Adicionalmente, el SST de una sesión de PDU ya establecida puede estar disponible en la entidad de 5GMM. Por lo tanto, la 5GMM puede usar también el o los SST de la sesión de la o las PDU asociadas con el intento de acceso. En resumen, la entidad de 5GMM puede obtener el o los SST  
5 relacionados con el intento de acceso de la entidad de 5GSM y/o de sí misma.

Además, pueden determinarse las categorías de acceso específicas de operador móvil o inalámbrico: La red proporciona al UE (entidad de 5GMM) con el filtro o filtros de categoría de acceso. El filtro está asociado con una categoría de acceso específica de operador y tiene una precedencia asociada en relación  
10 con categorías de acceso convencionales.

Determinación/relleno de configuración de prohibición por la BS:  
El NGAP (BS) puede determinar o rellenar la configuración de prohibición de acuerdo con la información de carga específica de segmento recibida de la red principal. La red principal puede indicar la carga específica de segmento en la  
15 red principal al nodo de RAN. La carga puede indicarse por PLMN, por SST, por SD, y/o por S-NSSAI.

La Figura 7 es un diagrama que ilustra un procedimiento global para prohibición de acceso para los intentos de acceso provocados por una capa superior de acuerdo con una implementación de ejemplo. La Figura 8 es un  
20 diagrama que ilustra un procedimiento global para prohibición de acceso para intentos de acceso activados por la capa de RRC de acuerdo con una implementación de ejemplo. La capa de RRC del UE en modo RRC-INACTIVO puede activar un intento de acceso. La capa de RRC puede recibir o no una categoría de acceso para el intento de acceso. En una implementación de  
25 ejemplo, la capa de NAS proporcionar una categoría de acceso para un mensaje

de NAS independientemente de los estados de RRC. La Figura 9 es un diagrama que ilustra un procedimiento para que un nodo de RAN establezca la configuración de prohibición para que se difunda de acuerdo con una implementación de ejemplo. La información de carga de la AMF y/o SMF por  
 5 segmento de red puede entregarse al nodo de RAN.

La Figura 10 es un diagrama que ilustra una técnica de prohibición de acceso específica de red de acuerdo con otra implementación de ejemplo. Las operaciones de 1 - 7 se describen a continuación, por medio de ejemplos ilustrativos.

10 1a. El cliente de IMS en el UE puede proporcionar al menos una de las siguientes indicaciones a la entidad de 5GMM en el UE ya sea directamente del cliente de IMS a la entidad de 5GMM o mediante la entidad de 5GSM:

- MO-MMTEL-iniciado por voz;
- MO-MMTEL-finalizado por voz;
- 15 - MO-MMTEL-iniciado por vídeo;
- MO-MMTEL-finalizado por vídeo;
- MO-SMSoIP-intento iniciado; y
- MO-SMSoIP-intento finalizado.

A partir de las indicaciones anteriores, la entidad de 5GMM puede tener  
 20 conocimiento del servicio de voz de MMTel de origen móvil, servicio de vídeo de MMTel y servicio de SMSoIP.

1b. La entidad de SMS del UE puede solicitar que la entidad de 5GMM entregue un mensaje de MO de SMS.

1c. La entidad de 5GSM del UE puede solicitar la entrega de mensaje de  
 25 5GSM a la entidad de 5GMM en el UE. Junto con el mensaje de 5GSM, la entidad

de 5GSM puede proporcionar también información de sesión de PDU, por ejemplo, ID de sesión de PDU, S-NSSAI, DNN.

La entidad de 5GMM puede almacenar la información proporcionada por la entidad de 5GSM además del mensaje de 5GSM, por ejemplo ID de sesión de PDU, S-NSSAI, DNN.

Si no se establece conexión de señalización de NAS de 5G para una sesión de PDU y necesitan entregarse datos de usuario de la sesión de PDU a la red, la entidad de 5GMM puede solicitarse que establezca una conexión de señalización de NAS de 5G por la entidad de control de flujo de QoS. En este caso, la entidad de 5GMM puede recibir también el ID de sesión de PDU de la sesión de PDU.

2. La red puede proporcionar el filtro o filtros de categoría de acceso específicos de operador a la entidad de 5GMM del UE mediante, por ejemplo, un mensaje de NAS, OMA DM. En caso de que el filtro o filtros de acceso específicos de operador se entreguen mediante un mensaje de NAS, es decir la AMF proporcionar el filtro o filtros al UE mediante un mensaje de 5GMM, el filtro o filtros puede provenir de la PCF. El mensaje de NAS puede corresponder al N1: mensaje de COMANDO DE ACTUALIZACIÓN DE CONFIGURACIÓN.

Cada uno de los filtros de categoría de acceso está asociado con una categoría de acceso específica de operador y/o valor de precedencia y puede incluir al menos uno de los siguientes criterios:

- SST; por segmento, y para uno o más tipos de servicio;
- SD;
- ID de aplicación;

- ID de SO;
- ID de aplicación de SO; y
- DNN.

Por ejemplo, en un tipo de segmento (o SST), podrían haber diferentes categorías de acceso para diferentes tipos de servicio (el ID de segmento puede ser, por ejemplo, una combinación de SST más SD, siendo SD opcional). Para cada combinación de SST+SD (o para cada segmento de red, donde el segmento puede asignarse a un tipo de servicio de los UE), puede haber una categoría de acceso. Un filtro de categoría de acceso puede indicar una categoría de acceso para cada uno de una pluralidad de segmentos (o para cada ID de segmento o SST). Esta información informa al UE cómo debe asignarse el intento de acceso a una categoría de acceso; esta categoría de acceso puede usarse por el UE para realizar análisis de prohibición de acceso: por ejemplo, un filtro (enviado al UE) para la categoría de acceso específica de operador X puede indicar que SST = eMBB y SD = Amazon, que significa que un intento de acceso sometido a un segmento de red de eMBB especializado para servicios de Amazon se clasificará como la categoría de acceso X. Como otro ejemplo, un filtro para la categoría de acceso específica de operador Y puede indicar esa DNN (nombre de red de datos, que podría estar vinculado al segmento, pero al mismo; Internet o subsistema multimedia de IMS/IP) = red empresarial, que significa que un intento de acceso sometido a tráfico empresarial interno debe estar categorizado como la categoría de acceso Y. Sometidos a la política del operador, los intentos de acceso categorizados como las categorías de acceso X e Y pueden priorizarse estableciendo valores pequeños de tasas de prohibición para estas categorías de acceso en la configuración de prohibición difundida.

El filtro o filtros de categoría de acceso específica de operador pueden tener una prioridad superior o inferior a las reglas de decisión de categoría de acceso normalizadas.

5 Como puede observarse a partir de los ejemplos anteriores, para proporcionar tratamiento especial para acceder a intentos relacionados con el tráfico propietario para los UE en itinerancia e incluso para los UE en la red doméstica (si la red desea cambiar la configuración anterior), la red deberá poder configurar el UE con categorías de acceso específicas de operador.

10 3. Teniendo en cuenta la información obtenida de la etapa 1 y la siguiente información disponible en la entidad de 5GMM:

- si el intento de acceso es una pregunta para un mensaje de terminación móvil;
- el o los SST de la sesión de la o las PDU asociadas con el intento de acceso (SST de una sesión de PDU ya establecida puede estar disponible en la 15 entidad de 5GMM);
- el PLMN del UE registrado y la o las HPLMN/EHPLMN/la o las VPLMN más preferidas del UE
- Cualquier categoría de acceso proporcionada por el operador que filtre el UE decide una categoría de acceso convencional. Los ejemplos de categorías 20 de acceso convencionales son:
  - MO resultante de MT: el intento de acceso es una respuesta a un mensaje de terminación móvil
  - voz de MO MMTel: el intento de acceso se provoca por un MO MMTel de llamada de voz
  - 25 - voz de MO MMTel: el intento de acceso se provoca por un MO MMTel de

llamada de vídeo

- MO SMSoIP: el intento de acceso se provoca por un MO SMSoIP
- MO SMSoNAS: el intento de acceso se provoca por un MO SMSoNAS
- MO emergencia: el intento de acceso es relevante para la llamada de  
5 emergencia
- servicio tolerante a retardo de MO en EHPLMN: el intento de acceso es relevante para el servicio tolerante a retardo o UE registrado en la EHPLMN del UE
- servicio tolerante a retardo de MO en la VPLMN más preferida: el intento  
10 de acceso es relevante para el servicio tolerante a retardo o UE registrado en la VPLMN más preferida del UE
- servicio tolerante a retardo de MO en otra PLMN: el intento de acceso es relevante para el servicio tolerante a retardo o UE registrado en otra PLMN
- MO eMBB: el intento de acceso es relevante para eMBB
- 15 - MO URLLC: el intento de acceso es relevante para URLLC
- señalización de MO: el intento de acceso no es para solicitud de recurso de radio de plano de usuario y no es relevante para otra categoría de acceso
- datos de MO: el intento de acceso es para la solicitud de recurso de radio de plano de usuario y no es relevante para otra categoría de acceso
- 20 - repliegue de VoLTE: el intento de acceso es para inicializar el repliegue de 5GS a voz sobre LTE en despliegues de red de 5GC tempranos

Hay casos donde un intento de acceso está asociado con múltiples SST. Para hacer frente a estos casos puede decidirse el orden de prioridad, por ejemplo URLLC > eMBB > IoT masivo, es decir, de nuevo, por ejemplo, se trata  
25 igual un intento de acceso asociado con URLLC y IoT masivo que con un intento

de acceso asociado con: URLLC y eMBB; o URLLC en solitario.

Además, si está disponible, el UE puede decidir que el intento de acceso está sometido a una categoría específica de operador teniendo en cuenta el filtro recibido en la etapa 2. Además de lo que la entidad de 5GMM considere como factores de entrada para la decisión de categoría de acceso para la categoría de acceso convencional, la entidad de 5GMM tiene en cuenta adicionalmente los parámetros que no se consideran como entrada para la decisión de categoría de acceso convencional, por ejemplo el o los SD relacionados con el intento de acceso.

10           4. La entidad de 5GMM de UE reenvía la categoría de acceso junto con el mensaje de NAS a la capa de RRC del UE.

5. La AMF (entidad de red principal de ejemplo) puede indicar la carga (carga de red global y cargas específicas de segmento) en la red principal al nodo/BS de RAN. La carga puede indicarse por PLMN, por SST, por SD, y/o por S-NSSAI. Tal información puede proporcionarse por la SMF al nodo de RAN. La información de carga puede expresarse en una escala de porcentaje por PLMN, por SST, por SD, y/o por S-NSSAI.

A) Más específicamente, la AMF puede proporcionar directamente su información de carga por PLMN, por SST, por SD, y/o por S-NSSAI al nodo de RAN. Puesto que los UE servidos por el nodo de RAN pueden servirse por múltiples AMF, el nodo de RAN puede necesitar recopilar información de carga de todas las AMF que sirven los UE servidos por el nodo de RAN, para figurar fuera de la carga global en la red principal (las AMF).

B) Por otra parte, la SMF puede proporcionar la información de carga por PLMN, por SST, por SD, y/o por S-NSSAI a la AMF, y la AMF puede reenviar la

información de carga al nodo de RAN. Puesto que los UE servidos por el nodo de RAN pueden servirse por múltiples SMF, el nodo de RAN puede necesitar recopilar información de carga de todas las SMF que sirven los UE servidos por el nodo de RAN, para figurar fuera de la carga global en la red principal (las SMF). En el mensaje de la AMF al nodo de RAN, la AMF puede incluir la información de carga de AMF por PLMN, por SST, por SD, y/o por S-NSSAI además de la información de carga de SMF que va a reenviarse.

C) o la AMF puede recoger información de carga por PLMN, por SST, por SD, y/o por S- NSSAI de las SMF y proporcionar la información de carga recogida al nodo de RAN. La información de carga recogida puede establecerse de modo que se refleja también la carga de la misma AMF además de la carga de SMF.

En B) y C), una SMF puede indicar los recursos asignados para un segmento de red con SST = IoT masivo como sobrecargados (por ejemplo el 98 % de carga). En B) la AMF reenvía la información de carga (los recursos de segmento de IoT masivo de SMF están el 98 % cargados), y en C) la AMF recupera información de carga de segmento de IoT masivo de la o las SMF y decide la carga de segmento de IoT masivo teniendo en cuenta también la carga de la AMF para el segmento de IoT masivo (en este caso, cómo calcula la AMF la carga global para el segmento de IoT masivo puede dejarse a la implementación).

6. El nodo de RAN rellena (determina) la configuración de prohibición por segmento (por ejemplo, que puede proporcionar prohibición superior para algunos segmentos, y tasas de prohibición inferiores para otros segmentos - priorización de algún tráfico sobre otro, por ejemplo, puede optar por tener una tasa de prohibición inferior para URLLC que para eMBB) que va a difundirse al

UE. A partir de la etapa 5, el nodo de RAN puede tener conocimiento del estado de carga de la red principal por PLMN, por SST, por SD y/o por S-NSSAI. Por lo tanto, el nodo de RAN puede rellenar o determinar la configuración de prohibición de modo que puede reducirse la carga para una PLMN/segmento de red particular, por ejemplo pueden establecerse los parámetros de prohibición para las categorías de acceso relacionadas con segmentos de red específicos (por ejemplo eMBB, URLLC, IoT masivo, IMS) de modo que se reduce el intento de acceso asociado con tales categorías de acceso. Obsérvese que el segmento de IoT masivo se mapea a categorías de acceso de series de servicios tolerantes a retardo.

La configuración de prohibición puede indicar uno o más de lo siguiente, por medio de ejemplo ilustrativo:

- si una clase o clases de acceso particulares deberían prohibirse con una cierta tasa de prohibición y temporizador de prohibición;
- si una categoría o categorías de acceso particulares deberían prohibirse con una cierta tasa de prohibición y temporizador de prohibición;
- si debe aplicarse prohibición para cada una de las clases de acceso en el intervalo 11-15;
- si la radiobúsqueda de nivel de RAN debe prohibirse con una cierta tasa de prohibición y temporizador de prohibición;
- parámetro o parámetros de compensación (por ejemplo para reducir la tasa de prohibición) para los UE de RRC-INACTIVO; y/o
- parámetro o parámetros de compensación (por ejemplo para reducir la tasa de prohibición) para sesiones de PDU de IMS de alta prioridad.

Obsérvese que la tasa de prohibición y el temporizador de prohibición para

los servicios de IMS (voz de MMTel, vídeo de MMTel, SMSoIP) y el parámetro o parámetros de compensación para sesiones de PDU de IMS de alta prioridad pueden entregarse al cliente de IMS en el UE por la capa de RRC en el UE y el cliente de IMS puede usar la información para comprobación de prohibición para

5 servicios de IMS.

Por ejemplo, un UE puede seleccionar un número aleatorio entre 0 y 1, y determina un factor de prohibición, y lo compara a la tasa de prohibición (si es menor que la tasa de prohibición, el intento de acceso no se prohíbe).

La implementación a modo de ejemplo de la configuración de prohibición  
10 difundida en información de sistema puede representarse como sigue:

**Elemento de información *SystemInformationBlockTypeX***

```

-- ASN1START

SystemInformationBlockTypeX ::= SEQUENCE {
    accessBarringConfiguration          SEQUENCE {
        plmn-identityIndex-r15         INTEGER (1..maxPLMN-r15)    OPTIONAL  -- Need OP
        abc-Info-r15                   SEQUENCE {
            abcForSpecialAC              BIT STRING (SIZE(5))    OPTIONAL  -- Need OP
            abcForAC                     BIT STRING (SIZE(10))    OPTIONAL  -- Need OP
            barringPerAccessCategoryList-r15 BarringPerAccessCategoryList-r15 OPTIONAL  --
Need OP
        }
        abcConfig-r15                  SEQUENCE {
            abcFactor-r15                ENUMERATED {
                p00, p05, p10, p15, p20, p25, p30, p40,
                p50, p60, p70, p75, p80, p85, p90, p95},
            abcTime-r15                  ENUMERATED {s4, s8, s16, s32, s64, s128, s256, s512}
        }
    }
    OPTIONAL  -- Need OP
}

BarringPerAccessCategory-r15 ::= SEQUENCE {
    accessCategory-r15                 INTEGER (1..maxAccessCategory-r15),
}

-- ASN1STOP

```

Cuando abc-Info-r15 pertenece a configuración colectiva de tres tipos de configuración de prohibición de acceso:

- para clases de acceso especiales (por ejemplo, AC11-15) por medio de  
5 abcForSpecialAC;
- para clases de acceso de LTE normales por medio de abcForAC;
- para categorías de acceso por medio del parámetro  
barringPerAccessCategoryList, donde el intervalo de categorías de acceso se  
determina por maxAccessCategory-r15.

10 Algunas ventajas a modo de ejemplo de diversas implementaciones de

ejemplo pueden incluir, o ejemplo, que la interfaz aérea y la capa de RRC del UE se vuelvan adaptables, extensibles y transparentes de alto grado \_\_en términos de suministro o prohibición de intentos de acceso particulares. Mientras que la NW (red) tiene los medios para controlar diversos servicios e intentos de acceso de terminal de la misma manera unificada. Suponiendo que la lista de categoría de acceso se define en la capa de RRC de una manera extensible, la técnica permite añadir potencialmente nuevos servicios sin la necesidad de cambiar la estructura de accesibilidad de servicio.

7. La capa de RRC del UE prohíbe intentos de acceso de acuerdo con la configuración de prohibición difundida, y la información sobre el intento de acceso, por ejemplo, al menos uno de lo siguiente, por ejemplo:

- categoría de acceso de la entidad de 5GMM;
- clase o clases de acceso del UE; y/o (no cubre el uso de las clases de acceso)
- si el intento de acceso está activando el cambio de RRC-INACTIVO a RRC-CONECTADO y, en caso afirmativo, si el intento de acceso se activa por radiobúsqueda de nivel de RAN.

Por ejemplo, si la entidad de 5GMM de un UE en el modo de RRC-INACTIVO solicitado la capa de RRC para transportar un mensaje de NAS con categoría de acceso = MO SMSoNAS y la configuración de prohibición indica que la tasa de prohibición para la categoría de acceso = MO SMSoNAS es el 40 % y el parámetro de compensación para el UE de RRC-INACTIVO es 0,3, el intento de acceso para el MO SMSoNAS debe prohibirse con una probabilidad de  $0,4 * 0,3 = 0,12$  (el 12 % de tal intento de acceso se prohibirá).

En una implementación de ejemplo, la capa de RRC de UE puede obtener

la clase o clases de acceso del UE de la USIM, pero si está no está disponible, la capa superior puede proporcionar la capa de RRC del UE con la clase o clases de acceso del UE.

- Si el intento de acceso para un UE en el modo de RRC-INACTIVO se
- 5 prohíbe, la capa de RRC debe indicar a la capa superior del resultado de prohibición con un caso específico. El caso debe indicar que el UE está prohibido debido a la configuración de prohibición del nodo de RAN de modo que este caso puede distinguirse del fallo de enlace de radio. En este caso, tanto en la capa de RRC como en la capa de NAS, el UE se vuelve al modo en espera. La capa de
- 10 NAS deberá operar como si el UE estuviera prohibido en el modo en espera.

Lista de abreviaturas de ejemplo:

|         |                                                           |
|---------|-----------------------------------------------------------|
| 3GPP    | proyecto de asociación de tercera generación              |
| 4G:     | cuarta generación de tecnología de telecomunicación móvil |
| 5G:     | quinta generación de tecnología de telecomunicación móvil |
| 5GMM:   | gestión de movilidad de 5GS                               |
| 5GS:    | sistema de 5G                                             |
| 5GSM:   | gestión de sesión de 5GS                                  |
| ACB:    | prohibición de clase de acceso                            |
| AMF:    | función de gestión de acceso y movilidad                  |
| CSFB:   | repliegue de conmutación de circuitos                     |
| DM:     | gestión de dispositivo                                    |
| DN:     | red de datos                                              |
| DNN:    | nombre de red de datos                                    |
| EHPLMN: | HPLMN equivalente                                         |
| eMBB:   | banda ancha móvil mejorada                                |

|          |                                                           |
|----------|-----------------------------------------------------------|
| eNB:     | nodo B evolucionado                                       |
| EPS:     | sistema de paquetes evolucionado                          |
| gNB:     | nodo B de la próxima generación (incierto)                |
| HPLMN    | PLMN doméstica                                            |
| IMS:     | subsistema multimedia de IP                               |
| IoT:     | Internet de las Cosas                                     |
| IP:      | protocolo de Internet                                     |
| MME:     | entidad de gestión de movilidad                           |
| MMTel:   | servicio de telefonía multimedia de IMS                   |
| NAS:     | estrato de no acceso                                      |
| NGAP:    | protocolo de aplicación de la siguiente generación        |
| NSSAI:   | información de asistencia de selección de segmento de red |
| OAM:     | operaciones, administración y gestión                     |
| OMA:     | alianza móvil abierta                                     |
| OS:      | sistema operativo                                         |
| PCF:     | función de control de política                            |
| PDU:     | unidad de datos de protocolo                              |
| PLMN     | red móvil pública terrestre                               |
| RAN:     | red de acceso de radio                                    |
| RRC:     | control de recursos de radio                              |
| S-NSSAI: | NSSAI único                                               |
| SD:      | diferenciador del segmento                                |
| SMS:     | servicio de mensajes cortos                               |
| SMSoNAS: | SMS sobre NAS                                             |
| SMSoIP:  | SMS sobre IP                                              |

|        |                                              |
|--------|----------------------------------------------|
| SSAC:  | control de acceso específico de servicio     |
| SST:   | tipo de segmento/servicio                    |
| UDM:   | gestión de datos de usuario                  |
| UE:    | equipo de usuario                            |
| UPF:   | función de plano de usuario                  |
| URLLC: | comunicación ultra-fiable y de baja latencia |
| VPLMN: | PLMN visitada                                |

La Figura 11 es un diagrama de bloques de una estación inalámbrica (por ejemplo, AP, BS, eNB, UE o dispositivo de usuario) 1100 de acuerdo con una implementación de ejemplo. La estación 1100 inalámbrica puede incluir, por ejemplo, uno o dos transceptores inalámbricos de RF (frecuencia de radio) 1102A, 1102B, donde cada transceptor inalámbrico incluye un transmisor para transmitir señales y un receptor para recibir señales. La estación inalámbrica también incluye un procesador o unidad/entidad de control (controlador) 1104 para ejecutar instrucciones o software y controlar la transmisión y recepciones de señales, y una memoria 1106 para almacenar datos y/o instrucciones.

El procesador 1104 puede también hacer decisiones o determinaciones, generar tramas, paquetes o mensajes para transmisión, decodificar tramas recibidas o mensajes para procesamiento adicional, y otras tareas o funciones descritas en el presente documento. El procesador 1104, que puede ser un procesador de banda base, por ejemplo, puede generar mensajes, paquetes, tramas u otras señales para su transmisión mediante el transceptor 1102 inalámbrico (1102A o 1102B). El procesador 1104 puede controlar la transmisión de señales o mensajes a través de una red inalámbrica, y puede controlar la recepción de señales o mensajes, etc., mediante una red inalámbrica (por

ejemplo, después de convertirse de manera descendente por el transceptor 1102 inalámbrico, por ejemplo). El procesador 1104 puede ser programable y puede ejecutar software u otras instrucciones almacenadas en memoria o en otros medios informáticos para realizar las diversas tareas y funciones anteriormente  
5 descritas, tal como una o más de las tareas o métodos anteriormente descritos. El procesador 1104 puede ser (o puede incluir), por ejemplo, hardware, lógica programable, un procesador programable que ejecuta software o firmware, y/o cualquier combinación de estos. Usando otra terminología, el procesador 1104 y el transceptor 1102 juntos pueden considerarse como un transmisor  
10 inalámbrico/sistema de receptor, por ejemplo.

Además, haciendo referencia a la Figura 11, un controlador (o procesador) 1108 puede ejecutar software e instrucciones, y puede proporcionar control global para la estación 1100, y puede proporcionar control para otros sistemas no mostrados en la Figura 11, tal como control de dispositivos de entrada/salida  
15 (por ejemplo, pantalla, teclado numérico), y/o puede ejecutar software para una o más aplicaciones que pueden proporcionarse en la estación 1100 inalámbrica, tal como, por ejemplo, un programa de correo electrónico, aplicaciones de audio/vídeo, un procesador de textos, una aplicación de voz sobre IP, u otra aplicación o software.

20 Además, puede proporcionarse un medio de almacenamiento que incluye instrucciones almacenadas, que cuando se ejecutan por un controlador o procesador pueden dar como resultado que el procesador 1104, u otro controlador o procesador, realicen una o más de las funciones o tareas anteriormente descritas.

25 De acuerdo con otra implementación de ejemplo, el transceptor o

transceptores 1102A/1102B de RF o inalámbricos pueden recibir señales o datos y/o transmitir o enviar señales o datos. El procesador 1104 (y posiblemente los transceptores 1102A/1102B) puede controlar el transceptor 1102A o 1102B de RF o inalámbrico para recibir, enviar, difundir o transmitir señales o datos.

5 Las realizaciones no están restringidas, sin embargo, al sistema que se proporciona como un ejemplo, sino que un experto en la materia puede aplicar la solución a otros sistemas de comunicación. Otro ejemplo de un sistema de comunicaciones adecuado es el concepto 5G. Se supone que la arquitectura de red en 5G será bastante similar a la de la LTE avanzada. 5G es probable que  
10 use antes de múltiple entrada - múltiple salida (MIMO), muchas más estaciones base o nodos que la LTE (un denominado concepto de célula pequeña), incluyendo macro sitios que operan en cooperación con estaciones más pequeñas y tal vez que también emplean diversas tecnologías de radio para mejor cobertura y tasas de datos potenciadas.

15 Debería apreciarse que las redes futuras probablemente utilizarán virtualización de funciones de red (NFV) que es un concepto de arquitectura de red que propone virtualizar funciones de nodo de red en "bloques de creación" o entidades que pueden estar operacionalmente conectadas o vinculadas juntas para proporcionar servicios. Una función de red virtualizada (VNF) puede  
20 comprender una o más máquinas virtuales que ejecutan códigos de programa informático usando servidores de tipo convencional o general en lugar de hardware personalizado. Puede utilizarse también informática en la nube o almacenamiento de datos. En comunicaciones de radio esto puede significar que se lleven a cabo operaciones de nodo, al menos parcialmente, en un servidor,  
25 anfitrión o nodo operacionalmente acoplado a una cabecera de radio remota.

También es posible que las operaciones del nodo se interrumpan entre una pluralidad de servidores, nodos o anfitriones. Debería entenderse también que la distribución del trabajo entre las operaciones de red principal y las operaciones de estación base pueden diferir de la LTE o incluso ser no existentes.

5 Las implementaciones de las diversas técnicas descritas en el presente documento pueden implementarse en circuitería electrónica digital, o en hardware, firmware, software informático o en combinaciones de los mismos. Las implementaciones pueden implementarse como un producto de programa informático, es decir, un programa informático incorporado de manera tangible  
10 en un soporte de información, por ejemplo, en un dispositivo de almacenamiento legible por máquina o en una señal propagada, para su ejecución por, o para controlar la operación de, un aparato de procesamiento de datos, por ejemplo, un procesador programable, un ordenador, o múltiples ordenadores. Las implementaciones pueden proporcionarse también en un medio legible por  
15 ordenador o medio de almacenamiento legible por ordenador, que puede ser un medio no transitorio. Las implementaciones de las diversas técnicas pueden incluir también implementaciones proporcionadas mediante señales transitorias o medios, y/o programas y/o implementaciones de software que pueden descargarse mediante Internet u otra red o redes, ya sean redes alámbricas y/o  
20 redes inalámbricas. Además, pueden proporcionarse implementaciones mediante comunicaciones de tipo máquina (MTC), y también mediante Internet de las Cosas (IOT).

El programa informático puede estar en forma de código fuente, forma de código objeto, o en alguna forma intermedia, y puede almacenarse en alguna  
25 clase de soporte, medio de distribución, o medio legible por ordenador, que

puede ser cualquier entidad o dispositivo apto para llevar el programa. Tales soportes incluyen un medio de grabación, memoria informática, memoria de solo lectura, señales fotoeléctricas y/o de portadora eléctrica, señal de telecomunicaciones, y paquete de distribución de software, por ejemplo.

- 5 Dependiendo de la potencia de procesamiento necesaria, el programa informático puede ejecutarse en un único ordenador digital electrónico o puede distribuirse entre un número de ordenadores.

Adicionalmente, las implementaciones de las diversas técnicas descritas en el presente documento pueden usar un sistema cibernético-físico (CPS) (un  
10 sistema de colaboración de elementos computacionales que controla entidades físicas). CPS puede posibilitar la implementación y aprovechamiento de cantidades masivas de dispositivos de ICT interconectados (sensores, accionadores, procesadores microcontroladores,...) embebidos en objetos físicos en diferentes localizaciones. Los sistemas físicos cibernéticos móviles, en  
15 los que el sistema físico en cuestión tiene movilidad intrínseca, son una subcategoría de sistemas cibernéticos-físicos. Ejemplos de sistemas físicos móviles incluyen robótica móvil y electrónica transportada por seres humanos o animales. El aumento en popularidad de los teléfonos inteligentes ha aumentado el interés en el área de sistemas cibernéticos-físicos móviles. Por lo tanto,  
20 pueden proporcionarse diversas implementaciones de técnicas descritas en el presente documento mediante una o más de estas tecnologías.

Un programa informático, tal como el programa o programas informáticos anteriormente descritos, pueden escribirse en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, y puede  
25 desplegarse en cualquier forma, incluyendo como un programa independiente o

como un módulo, componente, subrutina, u otra unidad o parte de ella adecuada para su uso en un entorno informático. Un programa informático puede desplegarse para ejecutarse en un ordenador o en múltiples ordenadores en un sitio o distribuirse a través de múltiples sitios e interconectarse por una red de comunicación.

Las etapas de método pueden realizarse por uno o más procesadores programables que ejecutan un programa informático o porciones de programa informático para realizar funciones operando en datos de entrada y generando salida. También pueden realizarse etapas de método por, y un aparato puede implementarse como, circuitería de lógica de fin especial, por ejemplo, un FPGA (campo de matriz de puertas programables) o un ASIC (circuito integrado específico de la aplicación).

Los procesadores adecuados para la ejecución de un programa informático incluyen, a modo de ejemplo, tanto microprocesadores de fin general como especial, y uno o más procesadores cualesquiera de cualquier clase de ordenador, chip o conjunto de chips digital. En general, un procesador recibirá instrucciones y datos de una memoria de solo lectura o una memoria de acceso aleatorio o ambas. Los elementos de un ordenador pueden incluir al menos un procesador para ejecutar instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. En general, un ordenador también puede incluir, o estar operativamente acoplado para recibir datos o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, discos magnéticos, discos magneto-ópticos u ópticos. Los soportes de información adecuados para realizar instrucciones de programa informático y datos incluyen todas las formas de memoria no volátil, incluyendo

a modo de ejemplo dispositivos de memoria de semiconductores, por ejemplo, EPROM, EEPROM, y dispositivos de memoria flash; discos magnéticos, por ejemplo, discos duros internos o discos extraíbles; discos magnetoópticos; y discos CD-ROM y DVD-ROM. El procesador y la memoria pueden  
5 complementarse por, o incorporarse en, circuitería de lógica de fin especial.

Para proporcionar interacción con un usuario, pueden implementarse implementaciones en un ordenador que tiene un dispositivo de visualización, por ejemplo, un tubo de rayos catódicos (CRT) o monitor de pantalla de cristal líquido (LCD), para visualizar información al usuario y una interfaz de usuario, tal como  
10 un teclado y un dispositivo apuntador, por ejemplo, un ratón o una bola de mando, mediante la cual el usuario puede proporcionar entrada al ordenador. Otros tipos de dispositivos pueden usarse para proporcionar interacción con un usuario también; por ejemplo, la realimentación proporcionada al usuario puede ser cualquier forma de realimentación sensorial, por ejemplo, realimentación  
15 visual, realimentación auditiva o realimentación táctil; y la entrada del usuario puede recibirse en cualquier forma, incluyendo acústica, voz o entrada táctil.

Las implementaciones pueden implementarse en un sistema informático que incluye un componente de extremo trasero, por ejemplo, como un servidor de datos, o que incluye un componente de soporte intermedio, por ejemplo, un  
20 servidor de aplicación, o que incluye un componente de extremo frontal, por ejemplo, un ordenador cliente que tiene una interfaz de usuario gráfica o un explorador web a través del cual un usuario puede interactuar con una implementación, o cualquier combinación de tales componentes de extremo trasero, soporte intermedio, o extremo frontal. Los componentes pueden  
25 interconectarse mediante cualquier forma o medio de comunicación de datos

digital, por ejemplo, una red de comunicación. Ejemplos de las redes de comunicación incluyen una red de área local (LAN) y una red de área extensa (WAN), por ejemplo, Internet.

Aunque se han ilustrado ciertas características de las implementaciones  
5 descritas como se describe en el presente documento, muchas modificaciones, sustituciones, cambios y equivalentes se les ocurrirá a los expertos en la materia. Ha de entenderse, por lo tanto, que las reivindicaciones adjuntas se pretende que cubran todas tales modificaciones y cambios como que caen dentro del espíritu verdadero de las diversas realizaciones.  
10

## **REIVINDICACIONES**

1. Un método que comprende:
  - detectar, por un dispositivo de usuario, un segmento de red o una  
5 aplicación asociados a un intento de acceso por el dispositivo de usuario para  
acceder a una red inalámbrica;
  - determinar, por el dispositivo de usuario, una categoría de acceso  
basándose en el segmento de red detectado o en la aplicación detectada; y
  - tomar, por el dispositivo de usuario, una decisión de prohibición para el  
10 intento de acceso basándose en la categoría de acceso determinada.
2. Un método de la reivindicación 1, en donde la toma de una decisión de  
prohibición comprende:
  - tomar, por el dispositivo de usuario basándose en la categoría de acceso  
15 determinada, una decisión que el intento de acceso no está prohibido; y
  - comprendiendo el método adicionalmente, por el dispositivo de usuario  
basándose en la decisión, el intento de acceso detectado a la red inalámbrica.
3. El método de la reivindicación 2, en donde la realización del intento de  
20 acceso detectado comprende:
  - enviar, por el dispositivo de usuario, un mensaje de solicitud de conexión  
de control de recursos de radio (RRC) para solicitar una conexión a la red  
inalámbrica.
- 25 4. El método de cualquiera de las reivindicaciones 1-3 y que comprende

adicionalmente:

recibir, por el dispositivo de usuario, un mensaje de estrato de no acceso que indica una respectiva categoría de acceso asociada a una o más aplicaciones; y

5            en donde determinar la categoría de acceso basándose en la aplicación detectada incluye:

determinar, por el dispositivo de usuario, la categoría de acceso para el intento de acceso basándose en la aplicación que está asociada al intento de acceso y la una o más definiciones de categoría de acceso.

10

5.        El método de cualquiera de las reivindicaciones 1-3 y que comprende adicionalmente:

recibir, por el dispositivo de usuario, una o más definiciones de categoría de acceso que indican una respectiva categoría de acceso asociada a uno o más  
15        segmentos de red; y

en donde determinar la categoría de acceso basándose en el segmento de red detectado incluye:

determinar, por el dispositivo de usuario, la categoría de acceso para el intento de acceso basándose en el segmento de red que está  
20        asociado al intento de acceso y la una o más definiciones de categoría de acceso.

6.        El método de cualquiera de las reivindicaciones 1-5, que comprende adicionalmente:

25        recibir, por el dispositivo de usuario, una configuración de prohibición que

indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso; y

en donde la toma de la decisión de prohibición para el intento de acceso incluye tomar, por el dispositivo de usuario, una decisión de prohibición para el intento de acceso basándose en la configuración de prohibición y la categoría de acceso para el intento de acceso.

7. El método de la reivindicación 6, en donde dicha configuración de prohibición indica si debe prohibirse una categoría de acceso particular con un cierto factor de prohibición y temporizador de prohibición, y en donde dicha toma de una decisión de prohibición para el intento de acceso basándose en la configuración de prohibición y la categoría de acceso para el intento de acceso comprende, cuando dicha configuración de prohibición indica que la categoría de acceso determinada debe prohibirse con un cierto factor de prohibición y tiempo de prohibición:

generar un número aleatorio; y

decidir que el intento de acceso no está prohibido cuando el número aleatorio es menor que el cierto factor de prohibición, de lo contrario decidir que el intento de acceso está al menos temporalmente prohibido.

20

8. El método de cualquiera de las reivindicaciones 6-7, en donde el conjunto de parámetros de prohibición incluye al menos una tasa de prohibición y un temporizador de prohibición.

25 9. El método de cualquiera de las reivindicaciones 6-8, en donde la

configuración de prohibición está basada en una información de carga específica de segmento de red que indica una carga de red para cada uno del uno o más segmentos de red.

- 5 10. El método de cualquiera de las reivindicaciones 6-9, en donde la configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso proporciona una priorización diferente de uno o más intentos de acceso basándose en las categorías de acceso de los intentos de acceso.
- 10 11. El método de cualquiera de las reivindicaciones 1-10, en donde el segmento de red asociado al intento de acceso se identifica por uno o más de lo siguiente:
  - un tipo de segmento/servicio (SST); y
  - 15 un tipo de segmento/servicio (SST) y un diferenciador de segmento (SD).
12. El método de cualquiera de las reivindicaciones 1-11, en donde la aplicación asociada al intento de acceso se identifica por uno o más de lo siguiente:
  - 20 identidad de sistema operativo; e
  - identidad de aplicación de sistema operativo.
13. El método de cualquiera de las reivindicaciones 1-12, y que comprende adicionalmente:
  - 25 recibir un parámetro de compensación para un dispositivo de usuario en

modo inactivo;

determinar, por el dispositivo de usuario, que el dispositivo de usuario está en modo inactivo; y

en donde la toma de una decisión de prohibición comprende:

- 5            aplicar, por el dispositivo de usuario, el parámetro de compensación a la toma de una decisión de prohibición para que el dispositivo de usuario ajuste una tasa de prohibición del intento de acceso del dispositivo de usuario que está en modo inactivo.

- 10    14.    Un método que comprende:

recibir, por una estación base de una o más entidades de red principales en una red inalámbrica, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red;

- 15            determinar, por la estación base basándose en la información de carga específica de segmento de red recibida, una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso; y

enviar, por la estación base a un dispositivo de usuario, la configuración de prohibición para reducir una carga en la red inalámbrica.

20

15.    El método de la reivindicación 14, en donde la configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso indica si un intento de acceso al que está asociado un segmento de red se activa por radiobúsqueda de nivel de red de acceso de radio (RAN).

25

16. El método de la reivindicación 15, en donde el envío comprende enviar, por la estación base a un dispositivo de usuario, la configuración de prohibición, para permitir que el dispositivo de usuario tome una decisión de prohibición para un intento de acceso basándose en un segmento de red asociado al intento de acceso por el dispositivo de usuario.
17. El método de cualquiera de las reivindicaciones 14-15, en donde el conjunto de parámetros de prohibición incluye al menos una tasa de prohibición y un temporizador de prohibición.
18. El método de cualquiera de las reivindicaciones 14 a 17, en donde dicha configuración de prohibición indica si debe prohibirse una categoría de acceso particular con un cierto factor de prohibición y temporizador de prohibición.
19. El método de cualquiera de las reivindicaciones 14-18, en donde el uno o más segmentos de red se identifican por uno o más de lo siguiente:
- un tipo de segmento/servicio (SST); y
  - un tipo de segmento/servicio (SST) y un diferenciador de segmento (SD).
20. Un método que comprende:
- determinar, por una entidad de red principal, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; y
  - enviar, por la entidad de red principal a una estación base, la información de carga específica de segmento de red.

21. El método de la reivindicación 20, donde la entidad de red principal comprende una primera entidad de red principal, y en donde la información de carga específica de segmento de red se determina por la primera entidad de red principal a partir de uno o más de lo siguiente:
- información de carga específica de segmento de red determinada o recogida por la primera entidad de red principal; y
  - información de carga específica de segmento de red recibida de una segunda entidad de red principal.
22. El método de cualquiera de las reivindicaciones 20-21 y que comprende adicionalmente:
- enviar, por la entidad de red principal a un dispositivo de usuario, una o más definiciones de categoría de acceso que indican una categoría de acceso asociada a uno o más segmentos de red.
23. El método de cualquiera de las reivindicaciones 20-22, en donde el uno o más segmentos de red se identifican por, o están asociados a uno o más de lo siguiente:
- un tipo de segmento/servicio (SST); y
  - un tipo de segmento/servicio (SST) y un diferenciador de segmento (SD).
24. Un dispositivo de usuario, que comprende,
- medios para detectar un segmento de red o una aplicación asociada con un intento de acceso por el dispositivo de usuario para acceder a una red

inalámbrica;

medios para determinar una categoría de acceso basándose en el segmento de red detectado o aplicación detectada; y

medios para tomar una decisión de prohibición para el intento de acceso  
5 basándose en la categoría de acceso determinada.

25. El dispositivo de usuario de la reivindicación 24, en donde los medios para tomar una decisión de realización de prohibición están configurados para tomar, basándose en la categoría de acceso determinada, una decisión de que el  
10 intento de acceso no está prohibido; y en donde el dispositivo de usuario comprende

medios para realizar, basándose en la decisión, el intento de acceso detectado a la red inalámbrica.

15 26. El dispositivo de usuario de la reivindicación 25, en donde los medios para realizar, basándose en la decisión, el intento de acceso detectado a la red inalámbrica están configurados para:

enviar un mensaje de solicitud de conexión de control de recursos de radio (RRC) para solicitar una conexión a la red inalámbrica.

20

27. El dispositivo de usuario de cualquiera de las reivindicaciones 24-26, que comprende adicionalmente:

medios para recibir un mensaje de estrato de no acceso que indica una respectiva categoría de acceso asociada con una o más aplicaciones; y

25 en donde dicha determinación de la categoría de acceso basándose en la

aplicación detectada incluye:

determinar la categoría de acceso para el intento de acceso basándose en la aplicación que está asociada con el intento de acceso y la una o más definiciones de categoría de acceso.

5

28. El dispositivo de usuario de cualquiera de las reivindicaciones 24-26, que comprende adicionalmente:

medios para recibir una o más definiciones de categoría de acceso que indican una respectiva categoría de acceso asociada con uno o más segmentos de red; y

10

en donde dicha determinación de la categoría de acceso basándose en el segmento de red detectado incluye:

determinar la categoría de acceso para el intento de acceso basándose en el segmento de red que está asociado con el intento de acceso y la una o más definiciones de categoría de acceso.

15

29. El dispositivo de usuario de cualquiera de las reivindicaciones 24-28, que comprende adicionalmente:

medios para recibir una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso; y

20

en donde dichos medios para tomar una decisión de prohibición para el intento de acceso basándose en la categoría de acceso determinada están configurados para tomar la decisión de prohibición basándose en la configuración de prohibición y la categoría de acceso para el intento de acceso.

25

30. El dispositivo de usuario de la reivindicación 29, en donde dicha configuración de prohibición indica si debe prohibirse una categoría de acceso particular con un cierto factor de prohibición y temporizador de prohibición, y en  
5 donde dichos medios para tomar una decisión de prohibición basándose en la categoría de acceso determinada están configurados para, cuando dicha configuración de prohibición indica que la categoría de acceso determinada debe prohibirse con un cierto factor de prohibición y tiempo de prohibición:
- generar un número aleatorio; y
- 10        decidir que el intento de acceso no está prohibido cuando el número aleatorio es menor que el cierto factor de prohibición, de lo contrario decidir que el intento de acceso está al menos temporalmente prohibido.
31. El dispositivo de usuario de cualquiera de las reivindicaciones 29-30, en  
15 donde el conjunto de parámetros de prohibición incluye al menos una tasa de prohibición y un temporizador de prohibición.
32. El dispositivo de usuario de cualquiera de las reivindicaciones 29-31, en  
20 donde la configuración de prohibición está basada en una información de carga específica de segmento de red que indica una carga de red para cada uno del uno o más segmentos de red.
33. El dispositivo de usuario de cualquiera de las reivindicaciones 30-32, en  
25 donde la configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más de las categorías de acceso proporciona una

priorización diferente de uno o más intentos de acceso basándose en las categorías de acceso de los intentos de acceso.

34. El dispositivo de usuario de cualquiera de las reivindicaciones 24-33, en  
5 donde el segmento de red asociado con el intento de acceso se identifica por uno o más de lo siguiente:

un tipo de segmento/servicio (SST); y

un tipo de segmento/servicio (SST) y diferenciador de segmento (SD).

10 35. El dispositivo de usuario de cualquiera de las reivindicaciones 24-34, en donde la aplicación asociada con el intento de acceso se identifica por uno o más de lo siguiente:

identidad de sistema operativo; e

identidad de aplicación de sistema operativo.

15

36. El dispositivo de usuario de cualquiera de las reivindicaciones 24-35, y que comprende adicionalmente:

medios para recibir un parámetro de compensación en modo inactivo;

20 medios para determinar que el dispositivo de usuario está en modo inactivo; y

en donde los medios para tomar una decisión de prohibición para el intento de acceso basándose en la categoría de acceso determinada están configurados para:

25 aplicar el parámetro de compensación a la toma de una decisión de prohibición para que el dispositivo de usuario ajuste una tasa de prohibición del

intento de acceso del dispositivo de usuario que está en modo inactivo.

37. Una estación base, que comprende:

5 medios para recibir de una o más entidades de red principales en una red inalámbrica, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red;

medios para determinar basándose en la información de carga específica de segmento de red recibida, una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso; y

10 medios para enviar a un dispositivo de usuario, la configuración de prohibición para reducir una carga en la red inalámbrica.

38. La estación base de la reivindicación 37, en donde la configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso indica si un intento de acceso con el que está asociado un  
15 segmento de red se activa por una radiobúsqueda de nivel de red de acceso de radio (RAN).

39. La estación base de la reivindicación 38, en donde los medios para envío  
20 están configurados para enviar a un dispositivo de usuario la configuración de prohibición, para permitir que el dispositivo de usuario tome una decisión de prohibición para un intento de acceso basándose en un segmento de red asociado con el intento de acceso por el dispositivo de usuario.

25 40. La estación base de cualquiera de las reivindicaciones 37 a 39, en donde

el conjunto de parámetros de prohibición incluye al menos una tasa de prohibición y un temporizador de prohibición.

41. La estación base de cualquiera de las reivindicaciones 37 a 40, en donde  
5 dicha configuración de prohibición indica si debe prohibirse una categoría de acceso particular con un cierto factor de prohibición y temporizador de prohibición.

42. La estación base de cualquiera de las reivindicaciones 37-41, en donde el  
10 uno o más segmentos de red se identifican por uno o más de lo siguiente:  
un tipo de segmento/servicio (SST); y  
un tipo de segmento/servicio (SST) y diferenciador de segmento (SD).

43. Una entidad de red principal, que comprende:  
15 medios para determinar información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red; y  
medios para enviar la información de carga específica de segmento de red a una estación base.

20 44. La entidad de red principal, donde la entidad de red principal comprende una primera entidad de red principal, y en donde la información de carga específica de segmento de red se determina por la primera entidad de red principal a partir de uno o más de lo siguiente:  
información de carga específica de segmento de red determinada o  
25 recogida por la primera entidad de red principal; e

información de carga específica de segmento de red recibida de una segunda entidad de red principal.

45. La entidad de red principal de cualquiera de las reivindicaciones 43-44, y  
5 que comprende adicionalmente:

medios para enviar una o más definiciones de categoría de acceso que indican una categoría de acceso asociada con uno o más segmentos de red a un dispositivo de usuario.

- 10 46. La entidad de red principal de cualquiera de las reivindicaciones 43-45, en donde el uno o más segmentos de red están identificados por o asociados con uno o más de lo siguiente:

un tipo de segmento/servicio (SST); y

un tipo de segmento/servicio (SST) y diferenciador de segmento (SD).

15

47. Un aparato que comprende al menos un procesador y al menos una memoria que incluye instrucciones informáticas que, cuando se ejecutan por el al menos un procesador, provocan que el aparato realice un método de cualquiera de las reivindicaciones 1-23.

20

48. Un aparato que comprende un producto de programa informático que incluye un medio de almacenamiento legible por ordenador no transitorio y que almacena código ejecutable que, cuando se ejecuta por al menos un aparato de procesamiento de datos, está configurado para provocar que el al menos un  
25 aparato de procesamiento de datos realice un método de cualquiera de las

reivindicaciones 1-23.

## **RESUMEN**

### **PROHIBICIÓN DE ACCESO ESPECÍFICO DE SEGMENTO DE RED PARA REDES INALÁMBRICAS**

5

Una técnica incluye detectar, por un dispositivo de usuario, un segmento de red asociado a un intento de acceso por el dispositivo de usuario para acceder a una red inalámbrica, y tomar, por el dispositivo de usuario, una decisión de prohibición para el intento de acceso basándose en el segmento de red asociado

10 al intento de acceso. Otro técnica de ejemplo puede incluir recibir, por una estación base de una o más entidades de red principales en una red inalámbrica, información de carga específica de segmento de red que indica una carga para cada uno del uno o más segmentos de red, determinar, por la estación base basándose en la información de carga específica de segmento de red recibida,

15 una configuración de prohibición que indica un conjunto de parámetros de prohibición para una o más categorías de acceso, y enviar, por la estación base a un dispositivo de usuario, la configuración de prohibición para reducir una carga en la red inalámbrica.

Red inalámbrica de ejemplo 130

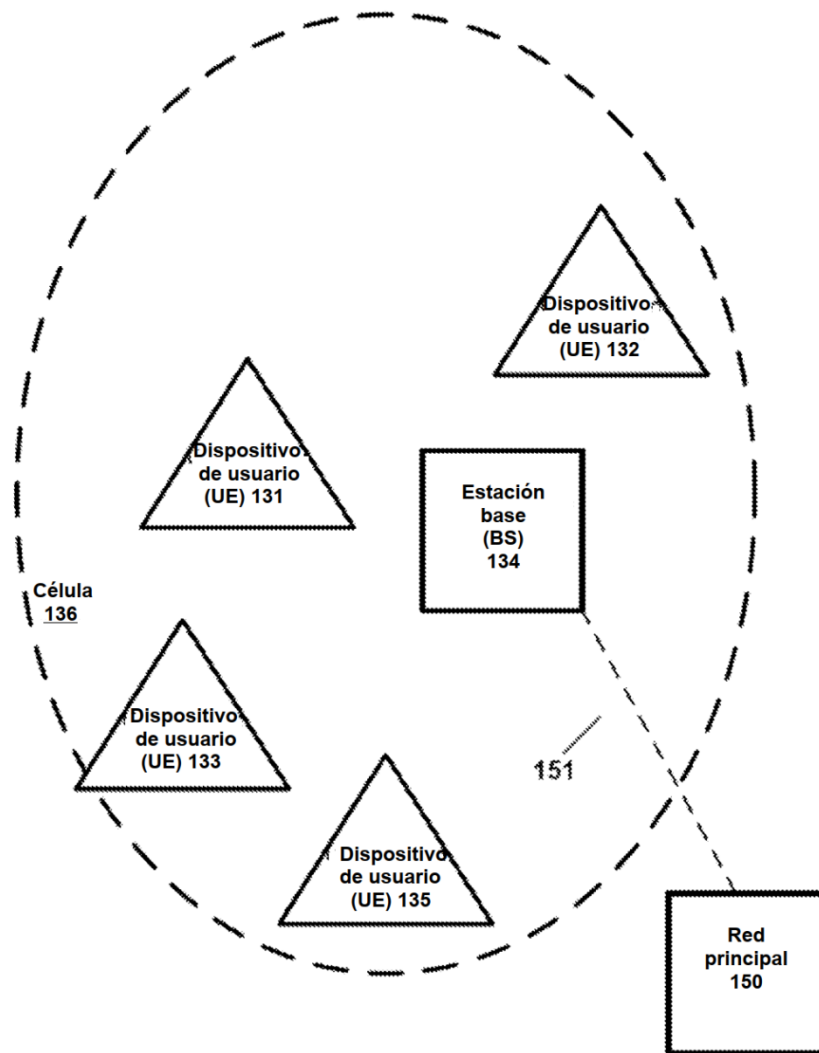


FIG. 1

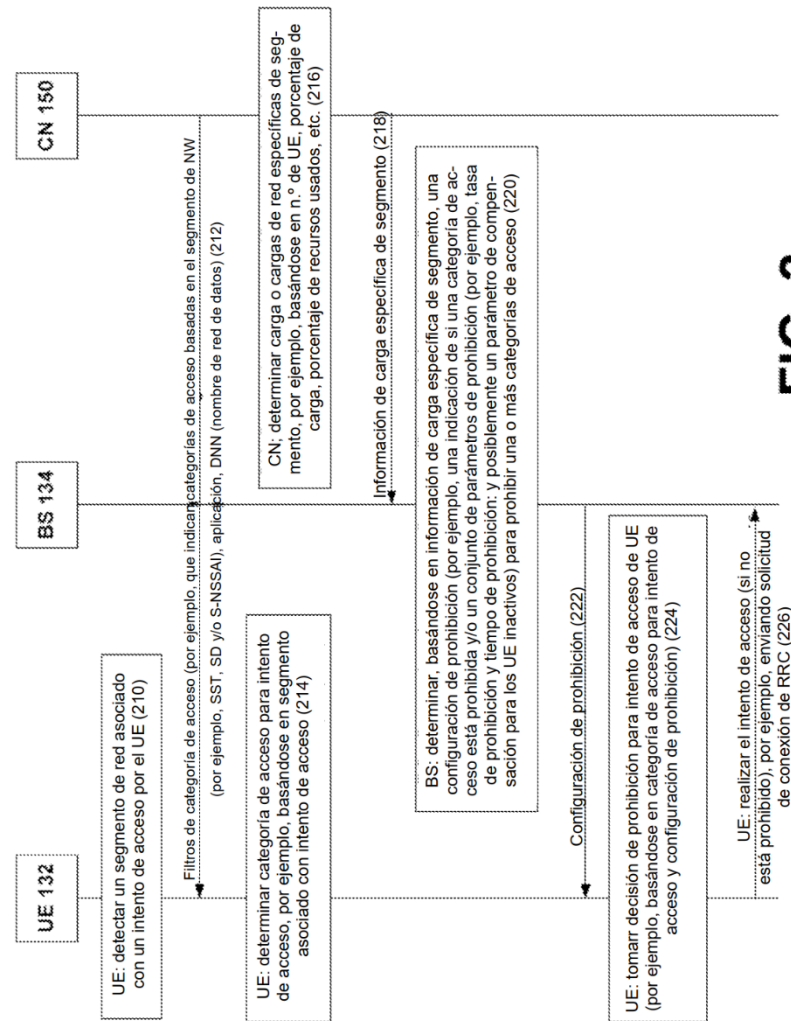


FIG. 2

67

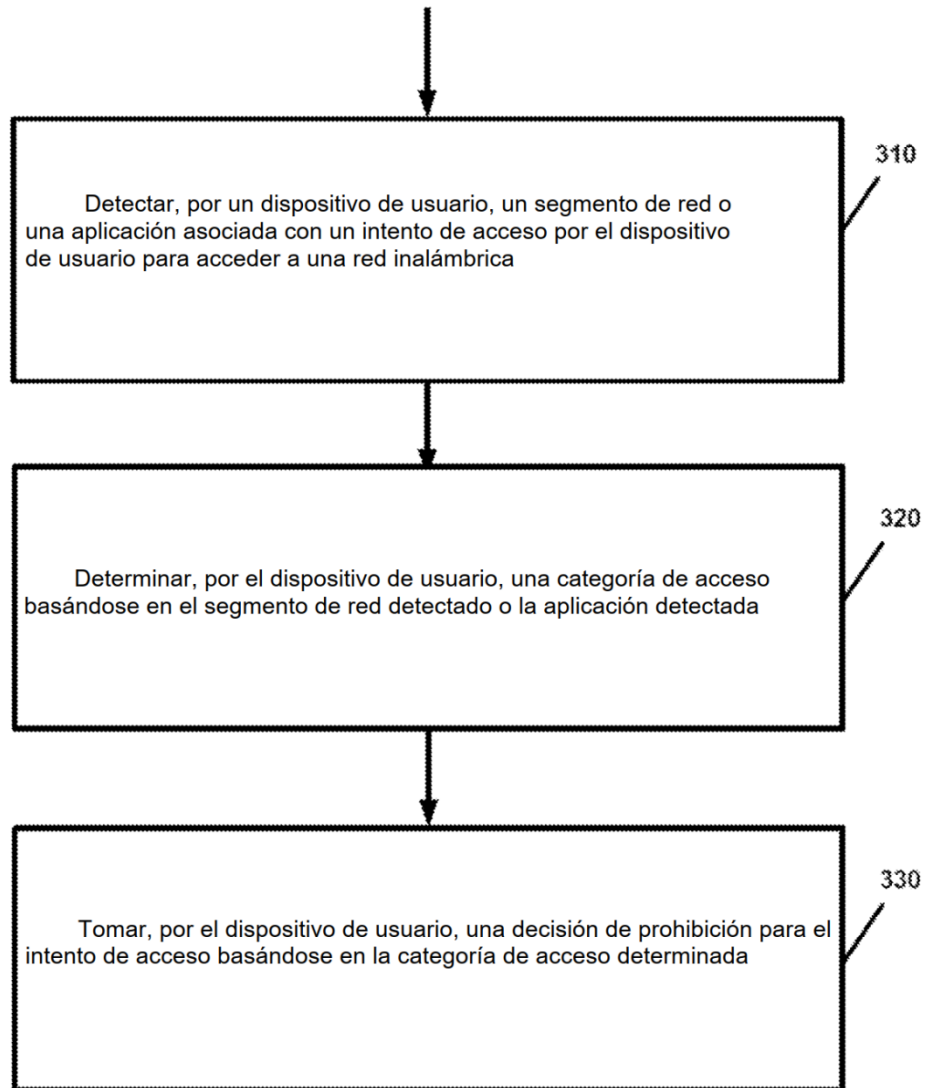


**FIG. 3**

68

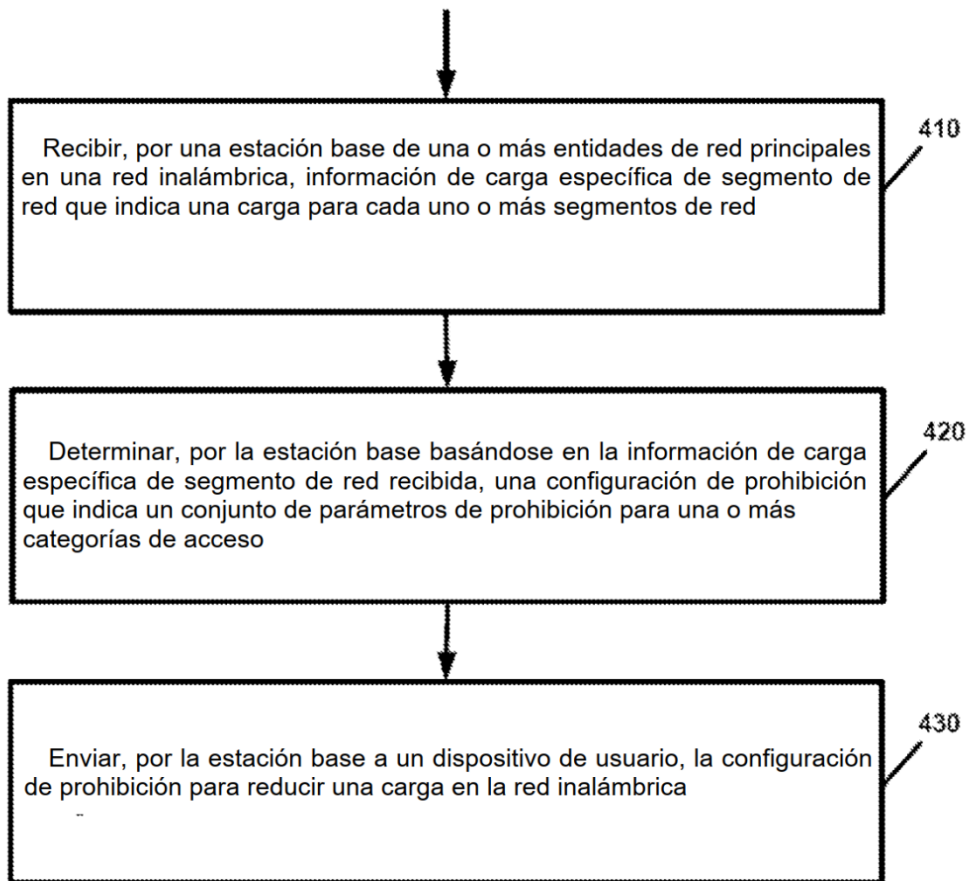


**FIG. 4**

69

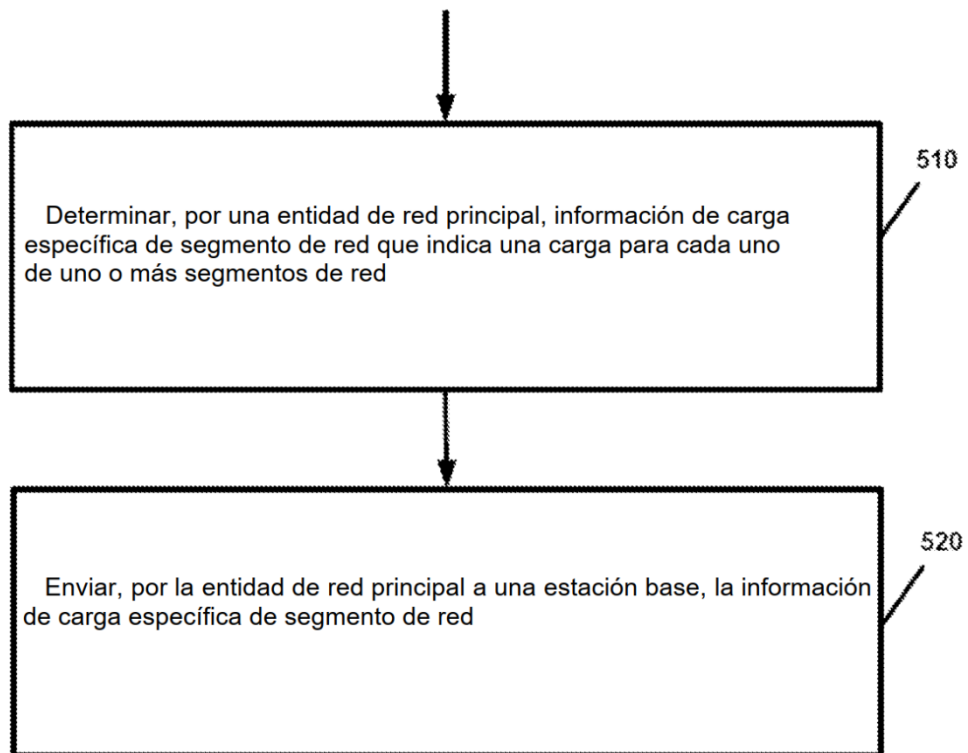
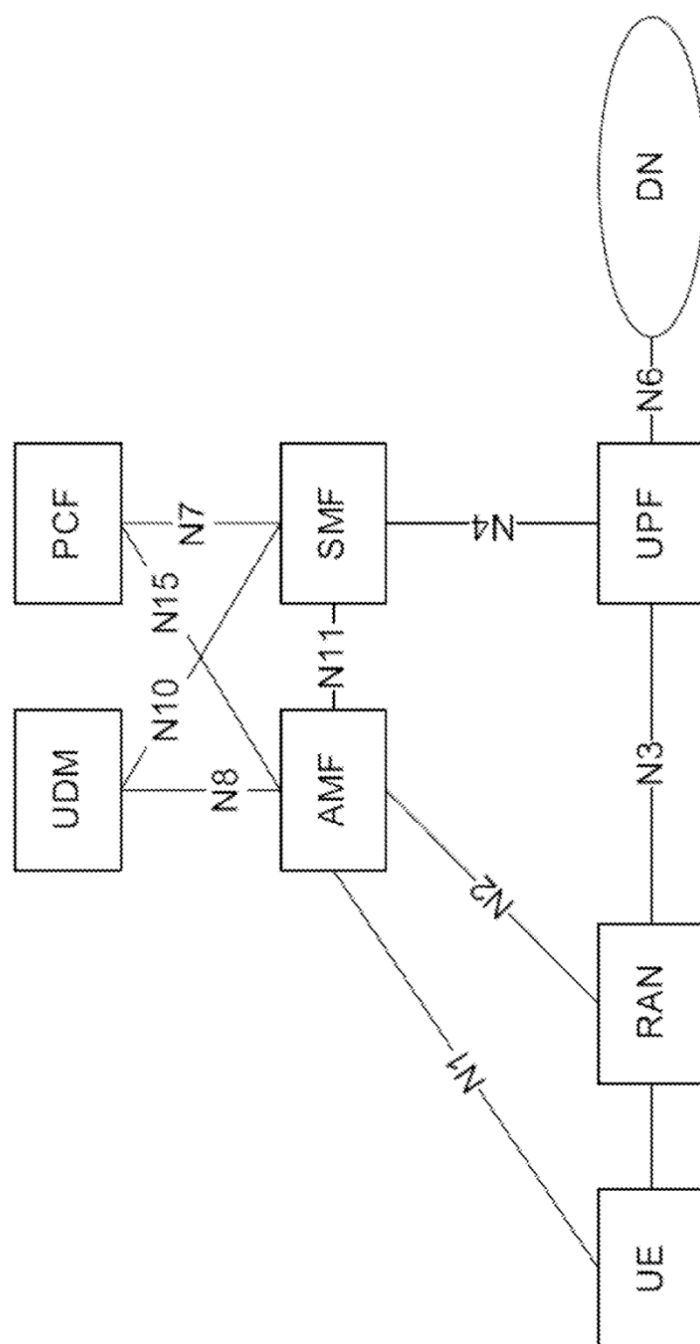
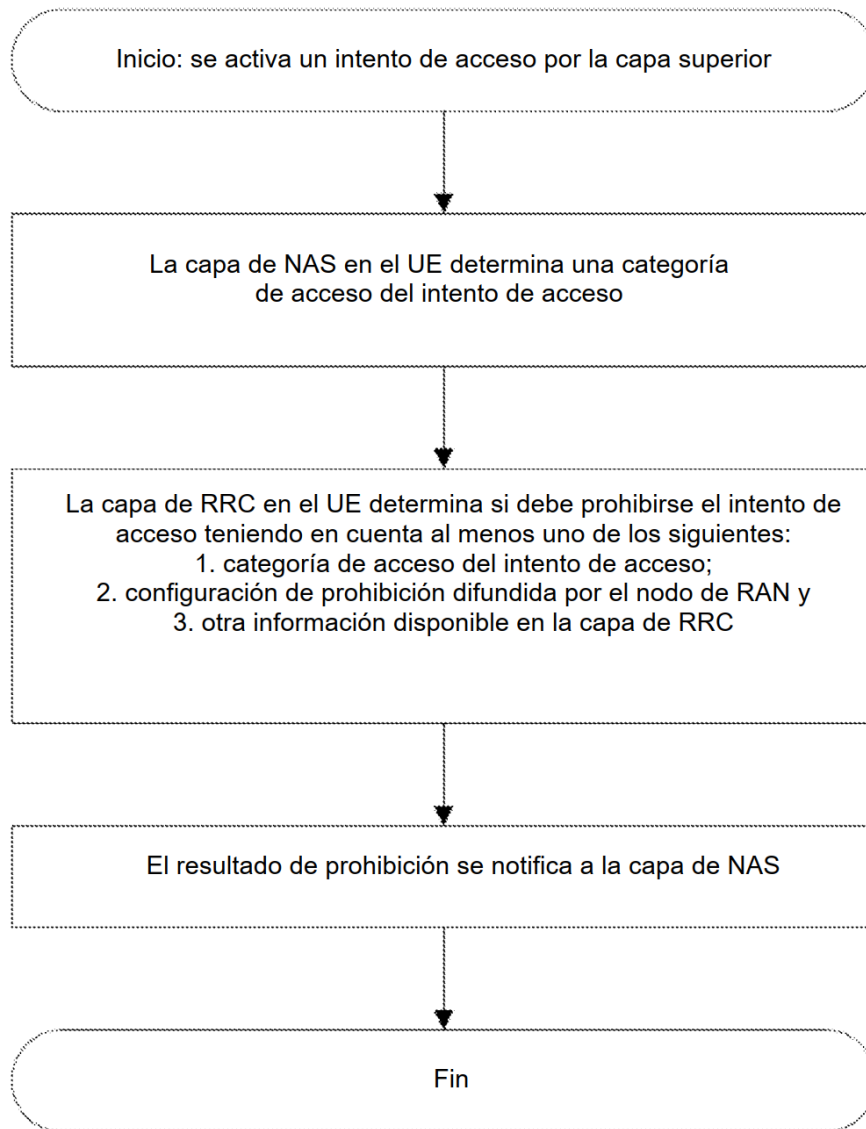
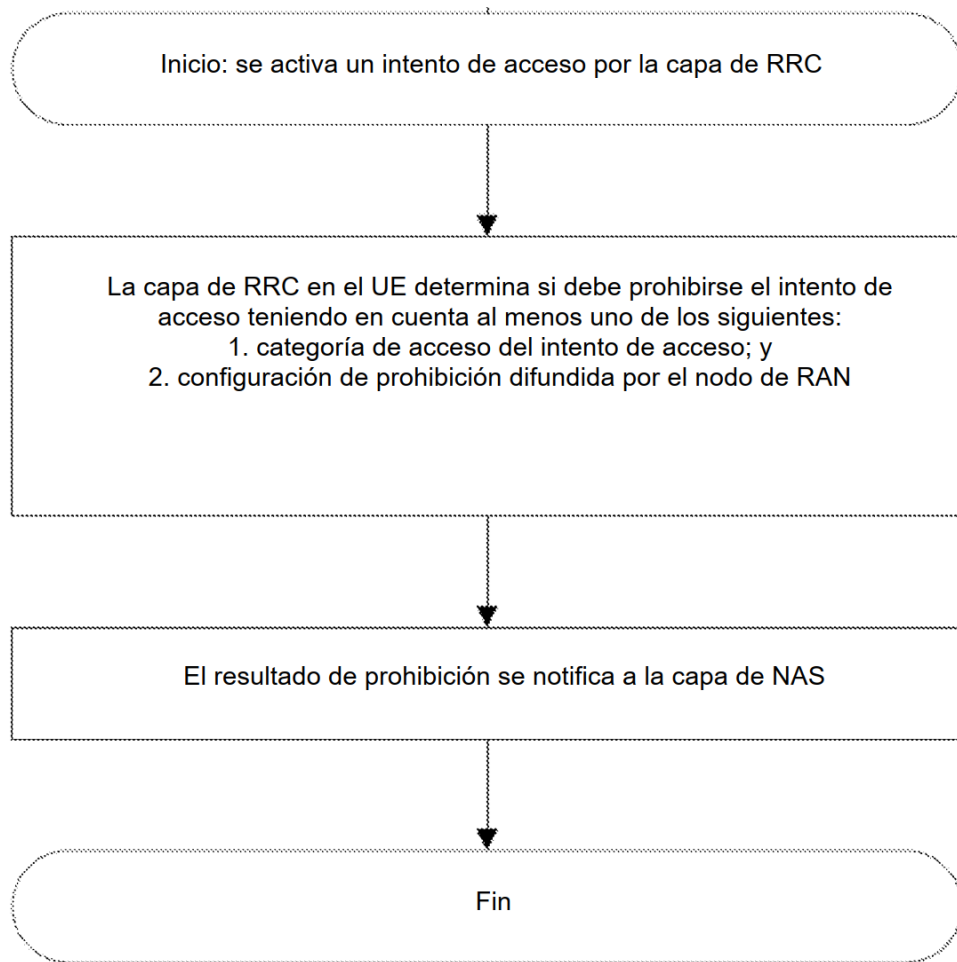
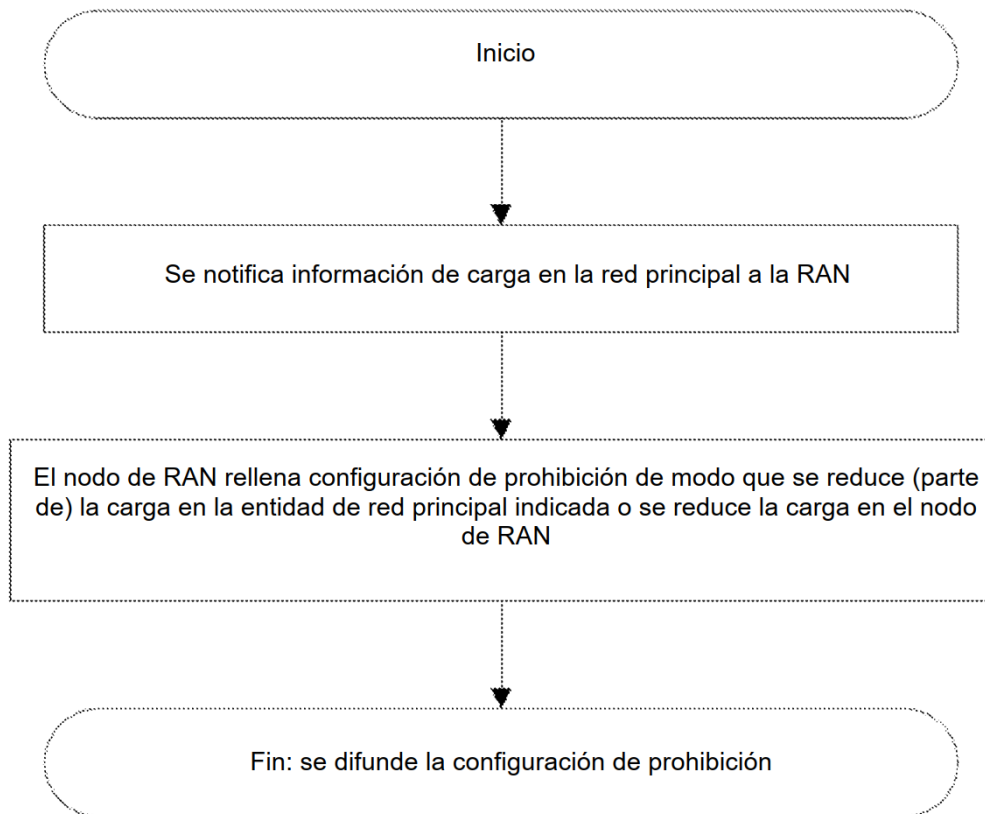


**FIG. 5**

**FIG. 6**

**FIG. 7**

**FIG. 8**

**FIG. 9**

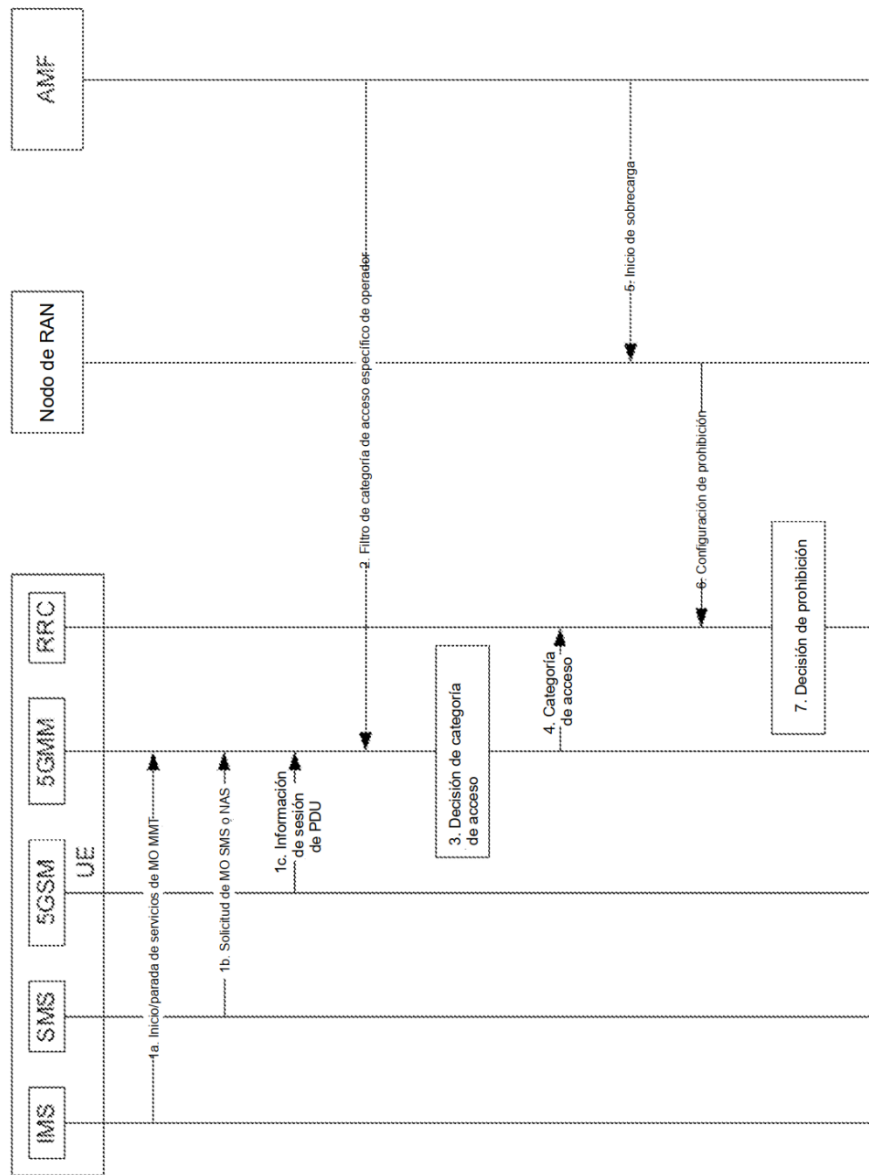
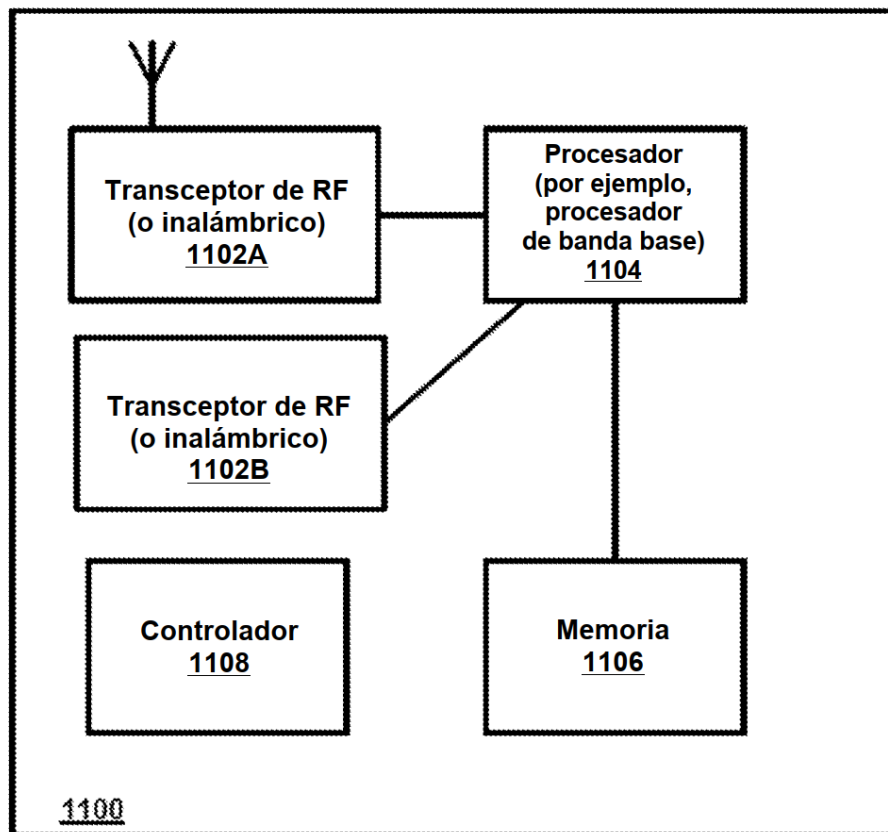


FIG. 10

**FIG. 11**