

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 765 862**

51 Int. Cl.:

H04W 12/12 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **20.01.2014 E 14151712 (8)**

97 Fecha y número de publicación de la concesión europea: **30.10.2019 EP 2760179**

54 Título: **Controlador del dispositivo de refuerzo de anclaje a red y métodos del mismo**

30 Prioridad:

29.01.2013 US 201313753405

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

11.06.2020

73 Titular/es:

**SYNCHRONOSS TECHNOLOGIES, INC. (100.0%)
200 Crossing Boulevard
Bridgewater, NJ 08807, US**

72 Inventor/es:

**VISHNUBHATT, PADDY;
SINGH, RAJESH;
TADURI, BALA K.;
BRATT, SANIDA y
PAUL, SUMEET**

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 765 862 T3

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

DESCRIPCIÓN

Controlador del dispositivo de refuerzo de anclaje a red y métodos del mismo

5 **Campo de la invención**

La presente invención se refiere a un controlador del dispositivo de refuerzo de anclaje a red y métodos del mismo.

10 **Antecedentes de la invención**

10 El anclaje a red se refiere al acoplamiento de un dispositivo de anclaje a red, como un ordenador, con un dispositivo de anclaje a red habilitado para Internet, tal como un teléfono inteligente, para que el dispositivo de anclaje a red pueda usar el servicio del plan de datos del dispositivo con acceso a Internet. El dispositivo anclado a red está configurado para comportarse como un módem, proporcionar acceso a Internet al dispositivo de anclaje a red. El acoplamiento entre el dispositivo de anclaje a red y el dispositivo anclado a red puede ser a través de un cable de datos, como un cable USB o un cable privado, o estar a través de LAN inalámbrica (Wi-Fi), a través de Bluetooth o un protocolo de comunicación privado, por citar unos pocos. El dispositivo anclado a red generalmente incluye una aplicación de anclaje a red para ofrecer acceso a Internet anclado a red. Una aplicación de anclaje a red puede ser una aplicación nativa proporcionada por el sistema operativo del dispositivo anclado a red y es compatible con OEM (fabricante original del teléfono).

25 La proliferación de teléfonos inteligentes y la gran cantidad de aplicaciones de anclaje a red disponibles actualmente han hecho que el anclaje a red sea cada vez más popular, especialmente ahora que muchos modelos de teléfonos son compatibles con aplicaciones de anclaje a red de terceros para acoplarse con dispositivos de anclaje a red a través de USB o por Bluetooth, o para crear puntos de acceso Wi-Fi (que a su vez brindan servicio a otros dispositivos en la vecindad/red). Las aplicaciones de anclaje a red habilitan el dispositivo anclado a red, por ejemplo, el teléfono inteligente, para compartir su acceso a Internet en cualquier lugar y en cualquier momento a otros dispositivos que de otro modo requerirían medios alternativos para acceder a Internet. La figura 1 ilustra un escenario de anclaje a red 100 a modo de ejemplo, que incluye un dispositivo anclado a red 105 y un dispositivo de anclaje a red 110. El dispositivo anclado a red 105 incluye normalmente una aplicación de anclaje a red para permitir compartir su conexión a Internet con el dispositivo de anclaje a red 110. Como se ilustra en la figura 1, el dispositivo anclado a red 105 es un teléfono inteligente y el dispositivo de anclaje a red 110 es un ordenador, y el acoplamiento entre el dispositivo anclado a red 105 y el dispositivo de anclaje a red 110 es a través de un cable USB 115.

35 El uso de teléfonos inteligentes como módems para que otros dispositivos accedan a Internet ha causado una seria preocupación para los operadores de telecomunicaciones a quienes no se contrata ni paga por el uso de sus redes móviles para que puedan acceder a ellos de manera que brinden servicios de Internet a ordenadores portátiles, ordenadores, tabletas o terceros usuarios. Los operadores inalámbricos luchan por mantener el uso del ancho de banda con la demanda. Los teléfonos inteligentes consumen mucho más ancho de banda que los teléfonos mejorados.

40 Los operadores inalámbricos están trabajando para bloquear el anclaje a red no autorizado o inapropiado, pero no han podido encontrar soluciones adecuadas para bloquear completamente el anclaje a red no autorizado a través de una aplicación de anclaje a red nativa o una aplicación de anclaje a red de terceros. Por ejemplo, los operadores inalámbricos están trabajando con empresas, como Google, y han podido bloquear algunas aplicaciones de anclaje a red de terceros, al filtrar aplicaciones de anclaje a red de terceros desde su portal o al bloquear la descarga de aplicaciones de anclaje a red de terceros del mercado(s) de aplicaciones en línea. Sin embargo, actualmente no hay una solución que pueda detectar, controlar y bloquear por completo la vinculación con aplicaciones de terceros, ya que los usuarios pueden cargar aplicaciones de terceros u obtener otra aplicación de vinculación del mercado que aún no ha pasado el escrutinio de los operadores inalámbricos. El mercado alberga múltiples aplicaciones y el número de tales aplicaciones aumenta cada día.

La presente invención aborda al menos estas limitaciones en la técnica anterior. Un ejemplo del estado de la técnica en el presente campo técnico se describe en el documento US 2012/240197 A1.

55 **Sumario de la invención**

La invención se define mediante las reivindicaciones independientes. Se definen realizaciones adicionales mediante las reivindicaciones dependientes.

60 Las realizaciones de la presente invención están dirigidas a un controlador de dispositivo de aplicación de anclaje a red y métodos del mismo. El controlador del dispositivo de aplicación de anclaje a red (TEDC) está instalado en un dispositivo primario, o también conocido como el dispositivo anclado a red. El TEDC está configurado para detectar, controlar y bloquear el anclaje a red no autorizada o inapropiada con un dispositivo secundario, o también conocido como dispositivo de anclaje a red, a través de una aplicación de anclaje a red nativa o de terceros, recuperando un archivo de configuración de un servidor asociado a un operador inalámbrico. El archivo de configuración generalmente incluye el perfil del cliente y los nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red

de terceros. El perfil del cliente generalmente incluye información de suscripción, incluido el uso de servicios de anclaje a red. Si el cliente está intentando el anclaje a red y el anclaje a red no está permitido, entonces el TEDC evitará que el anclaje a red del dispositivo secundario con el dispositivo primario. En algunas realizaciones, el TEDC es una aplicación de desanclaje de red instalada en el dispositivo primario.

5 En un aspecto, se proporciona un aparato. El aparato normalmente incluye una memoria no transitoria para almacenar instrucciones y un componente de procesamiento acoplado a la memoria. El componente de procesamiento generalmente está configurado para procesar las instrucciones.

10 Las instrucciones son normalmente para acceder a un archivo de configuración desde un servidor. En algunas realizaciones, el archivo de configuración se basa en servicios de suscripción de anclaje a red. En algunas realizaciones, el archivo de configuración incluye nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros. En algunas realizaciones, el archivo de configuración está en formato XML.

15 Las instrucciones también son normalmente para determinar el estado de suscripción de anclaje a red del aparato. Las instrucciones también son normalmente para, según el estado de la suscripción de anclaje a red, bloquear el anclaje a red con otro dispositivo.

20 En algunas realizaciones, las instrucciones también son para verificar si alguno de los valores en el archivo de configuración corresponde con una aplicación en ejecución en el aparato.

En algunas realizaciones, las instrucciones también son para verificar que se haya iniciado una aplicación de anclaje a red.

25 En algunas realizaciones, las instrucciones también son para escuchar una o más "transmisiones" por el aparato al acoplarse con el otro dispositivo.

En algunas realizaciones, las instrucciones también son para presentar un mensaje sobre el estado de la suscripción de anclaje a red.

30 En algunas realizaciones, las instrucciones también son para enviar datos preliminares al servidor. Los datos preliminares incluyen información de identificación del aparato.

35 En algunas realizaciones, las instrucciones también son para determinar todas las aplicaciones actualmente en vivo que se ejecutan en el aparato.

En algunas realizaciones, las instrucciones se invocan al arrancar el sistema operativo del aparato. Alternativamente, las instrucciones se invocan al anclar a red el aparato con el otro dispositivo.

40 En otro aspecto, se proporciona un medio legible por ordenador no transitorio. Un medio legible por ordenador no transitorio que almacena instrucciones que, cuando se ejecuta por un dispositivo informático, hacen que el dispositivo informático lleve a cabo un método. El método generalmente incluye enviar información de identificación a un servidor, recibir un archivo de configuración personalizado basado en la información de identificación, determinar si evocar una aplicación de anclaje a red y, basado en la determinación, comprobar la permisibilidad del anclaje a red. En algunas realizaciones, la verificación de la admisibilidad del anclaje a red incluye hacer referencia al archivo de configuración. El método también incluye desconectar el anclaje a red cuando no está permitido y permitir el anclaje a red cuando está permitido. En algunas realizaciones, desconectar el enlace incluye solicitar un mensaje.

50 En algunas realizaciones, cuando la aplicación de anclaje a red es una aplicación de anclaje a red de terceros, determinar si se invoca una aplicación de anclaje a red incluye escuchar una o más transmisiones por el dispositivo informático, generar una lista de paquetes que se ejecutan actualmente en el dispositivo informático y comparar la lista de paquetes que se ejecutan actualmente con una lista de nombres de paquetes de aplicaciones incluidos en la lista negra incluidos en el archivo de configuración.

55 En algunas realizaciones, cuando la aplicación de anclaje a red es una aplicación de anclaje a red nativa, determinar si se invoca una aplicación de anclaje a red incluye escuchar una o más transmisiones por el dispositivo informático y validar el anclaje a red.

60 En otro aspecto más, se proporciona un sistema de anclaje a red. El sistema de anclaje a red normalmente incluye una red, un servidor y un dispositivo primario. El servidor y el dispositivo primario están conectados comunicativamente con la red.

65 El servidor generalmente incluye perfiles de clientes y nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros. El servidor generalmente está configurado para generar archivos de configuración personalizados.

El dispositivo primario generalmente está configurado para proporcionar información de identificación al servidor y descargar un archivo de configuración personalizado del servidor. En algunas realizaciones, el archivo de configuración personalizado incluye perfiles de clientes y nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros. En algunas realizaciones, cada perfil de cliente incluye información de suscripción de vinculación con respecto al cliente respectivo.

Basado en al menos el archivo de configuración personalizado, el dispositivo primario también está configurado normalmente para no permitir y permitir el anclaje a red al detectar dicho anclaje a red. En algunas realizaciones, no permitir el anclaje a red es en respuesta a un anclaje a red incorrecto, y permitir el anclaje a red es en respuesta a un anclaje a red correcto. El anclaje a red puede ser a través de USB, punto de acceso Bluetooth o Wi-Fi.

Breve descripción de los dibujos

Ahora se hará referencia en detalle a las implementaciones de la presente invención como se ilustra en los dibujos adjuntos. Los mismos indicadores de referencia se usarán a lo largo de los dibujos y la siguiente descripción detallada para hacer referencia a las mismas partes o a partes similares.

La figura 1 ilustra un escenario de anclaje a red a modo de ejemplo.

La figura 2 ilustra un diagrama de bloques de un dispositivo de anclaje a red a modo de ejemplo de acuerdo con la presente invención.

La figura 3 ilustra un sistema de anclaje a red a modo de ejemplo de acuerdo con la presente invención.

La figura 4 ilustra un método de refuerzo de anclaje a red a modo de ejemplo general de acuerdo con la presente invención.

La figura 5 ilustra un método de refuerzo de anclaje a red a modo de ejemplo detallado de acuerdo con la presente invención.

La figura 6A ilustra una notificación a modo de ejemplo mostrada durante el período de prueba de acuerdo con la presente invención.

La figura 6B ilustra una notificación a modo de ejemplo mostrada bajo la categoría bloqueada de acuerdo con la presente invención.

Descripción detallada de la invención

En la siguiente descripción, se exponen numerosos detalles con fines de explicación. Sin embargo, un experto en la materia se dará cuenta de que la invención se puede practicar sin el uso de estos detalles específicos. Por lo tanto, la presente invención no pretende limitar las realizaciones mostradas, sino que debe acordarse el ámbito más amplio consistente con los principios y las características descritas en el presente documento.

Las realizaciones de la presente invención están dirigidas a un controlador de dispositivo de aplicación de anclaje a red y métodos del mismo. El controlador del dispositivo de aplicación de anclaje a red (TEDC) está instalado en un dispositivo primario, o también conocido como el dispositivo anclado a red. El TEDC está configurado para detectar, controlar y bloquear el anclaje a red no autorizada o inapropiada con un dispositivo secundario, o también conocido como dispositivo de anclaje a red, a través de una aplicación de anclaje a red nativa o de terceros, recuperando un archivo de configuración de un servidor asociado a un operador inalámbrico. El archivo de configuración generalmente incluye el perfil del cliente y los nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros. El perfil del cliente generalmente incluye información de suscripción, incluido el uso de servicios de anclaje a red. Si el cliente está intentando el anclaje a red y el anclaje a red no está permitido, entonces el TEDC evitará que el anclaje a red del dispositivo secundario con el dispositivo primario. En algunas realizaciones, el TEDC es una aplicación de desanclaje de red instalada en el dispositivo primario.

El TEDC puede ser instalado por el fabricante del dispositivo anclado a red o por la portadora inalámbricos y generalmente se instala antes de la venta del dispositivo anclado a red a un usuario. Preferentemente, el TEDC no se puede desinstalar. El TEDC generalmente se instala en el espacio del sistema del dispositivo anclado a red (por ejemplo, sistema/carpeta de la aplicación). Se puede invocar el TEDC al iniciar el sistema operativo del dispositivo anclado a red o al conectar el dispositivo anclado a red con un dispositivo de anclaje a red.

Dentro de esta discusión actual, "usuario", "suscriptor" y "cliente" son sinónimos y se usan indistintamente en este documento. También dentro de esta discusión, "portadora inalámbrica", "operador inalámbrico" y "proveedor de servicios" son sinónimos y se usan indistintamente en este documento.

La figura 2 ilustra un diagrama de bloques de un dispositivo anclado a red a modo de ejemplo 200 de acuerdo con la presente invención. El dispositivo anclado a red 200 se puede utilizar para adquirir, almacenar, calcular, procesar, comunicar y/o mostrar información. El dispositivo anclado a red 200 también puede acceder a una red, tal como Internet.

En general, una estructura de hardware adecuada para implementar el dispositivo anclado a red 200 incluye una interfaz de red 202, una memoria 204, un procesador 206, dispositivo(s) de E/S 208, un bus 210 y un dispositivo de

almacenamiento 212. La elección del procesador no es crítica siempre que se elija un procesador adecuado con suficiente velocidad. La memoria 204 puede ser cualquier memoria de ordenador convencional conocida en la técnica. El dispositivo de almacenamiento 212 puede incluir un disco duro, CD-ROM, CDRW, DVD, DVDRW, Blue-Ray®, tarjeta de memoria flash o cualquier otro dispositivo de almacenamiento. El dispositivo anclado a red 200 puede incluir una o más interfaces de red 202 para conectarse a una red celular, una Ethernet y/u otro tipo de LAN. Los dispositivos de E/S 208 pueden incluir uno o más de los siguientes: teclado, ratón, monitor, visualizador, impresora, módem, pantalla táctil, interfaz de botón y otros dispositivos. En algunas realizaciones, la estructura de hardware incluye múltiples procesadores y otro hardware para realizar el procesamiento en paralelo. La aplicación(es) 214, incluyendo el TEDC y una aplicación de anclaje a red, es probable que se almacenen en el dispositivo de almacenamiento 212 y la memoria 204 y se procesen a medida que se procesan las aplicaciones. Se pueden incluir más o menos componentes mostrados en la figura 2 en el dispositivo informático 200.

Los ejemplos de un dispositivo anclado a red adecuado incluyen un teléfono inteligente (por ejemplo, un iPhone®), una tableta (por ejemplo, un iPad®) o cualquier otro dispositivo informático adecuado capaz de recibir y enviar datos desde una red. El dispositivo anclado a red generalmente está suscrito a servicios de Internet proporcionados por un proveedor de servicios inalámbricos.

La figura 3 ilustra un sistema de anclaje a red 300 a modo de ejemplo de acuerdo con la presente invención. El sistema de anclaje a red 300 incluye una red 320. Un dispositivo anclado a red 305, como el dispositivo anclado a red 200 (figura 2), se conecta con la red utilizando los servicios de datos proporcionados por la portadora inalámbrica. Como se muestra en la figura 3, uno o más dispositivos de anclaje a red 310 están intentando anclar a red con el dispositivo de anclaje a red 305. El anclaje a red se puede hacer con un cable (por ejemplo, USB o serie) o de forma inalámbrica a través de Bluetooth, Wi-Fi u otros métodos inalámbricos como infrarrojos o IrDA. Un dispositivo de anclaje a red 310 puede ser un ordenador, un ordenador portátil, un dispositivo asistente digital personal, un teléfono inteligente, una tableta, o similar. Un dispositivo de anclaje a red 310 puede ser del mismo modelo y fabricación que el dispositivo de anclaje a red 305.

Un servidor(es) 315 asociado a la portadora inalámbrica también está acoplado con la red 320. El servidor 315 generalmente incluye perfiles de clientes y nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros. Cada perfil de cliente generalmente incluye información de suscripción de un cliente, incluido el uso de servicios de anclaje a red. Cada perfil de cliente generalmente es actualizado por el proveedor de servicios inalámbricos. El proveedor de servicios inalámbricos puede actualizar una lista de nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros y/o de forma independiente por otros. En algunas realizaciones, el servidor 325 está configurado para preparar datos de configuración apropiados para ser presentados a un cliente en un formato XML u otro formato adecuado.

Suponga que el TEDC ya está instalado e invocado en un dispositivo Android y que el usuario está intentando utilizar el dispositivo Android como dispositivo anclado a red. A efectos de esta descripción, se describe un dispositivo Android a modo de ejemplo. Será evidente que se pueden usar otros dispositivos como el dispositivo anclado a red. Una vez que se inicia el TEDC y hay Internet móvil disponible, como parte del inicio de sesión inicial con el servidor, el dispositivo Android está configurado para enviar datos preliminares, como el dispositivo MDN/CTN (número de dispositivo móvil/número de teléfono celular), IMEI (identidad internacional de equipos móviles), versión del sistema operativo (OS) y otra información del fabricante, al servidor. Al recibir los datos preliminares del usuario, el servidor revisa los datos preliminares y determina una categoría de vinculación del usuario. En algunas realizaciones, el usuario cae dentro de una de las tres categorías de anclaje a red, que son de prueba, bloqueado o permitido. Después de la revisión inicial por parte del servidor, el servidor genera un archivo XML para el usuario. El archivo XML generalmente contiene datos de configuración personal de acuerdo al menos con la categoría de anclaje a red del usuario. En algunas realizaciones, el usuario recibe un nuevo archivo de configuración del servidor en cada intento de anclaje a red.

En algunas realizaciones, un período de prueba es el período de tiempo que un proveedor de servicios inalámbricos permite a sus usuarios conectarse y notificará a los usuarios con notificaciones especiales sobre los estados de suscripción de prueba. Una condición bloqueada es cuando, después de la finalización del período de prueba, un usuario no se suscribe a un plan de servicio de anclaje a red y, en ese caso, en cada intento de anclaje a red posterior, el anclaje a red se bloquea, con o sin notificación, hasta que el usuario se suscriba a un plan de servicio de anclaje a red. Una condición permitida es cuando un usuario está suscrito a un plan de servicio de anclaje a red o ha indicado que el usuario desea suscribirse a un plan de servicio de anclaje a red después de la finalización del período de prueba.

La figura 4 ilustra un método de refuerzo de anclaje a red 400 a modo de ejemplo de acuerdo con la presente invención. El método 400 se produce después de que el dispositivo Android envía los datos preliminares al servidor. Los datos preliminares generalmente incluyen información de identificación del dispositivo Android. En algunas realizaciones, el método 400 se produce después de que el dispositivo Android está acoplado al ordenador. El método 400 se inicia en la etapa 405, en la que un archivo de configuración personalizado es generado y recuperado del servidor. El servidor generalmente está asociado a la portadora inalámbrica. El archivo de configuración, que incluye el perfil del cliente del usuario, la lista de nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje

a red de terceros y/u otra información como mensajes de aviso, se descarga automáticamente en el dispositivo Android.

5 En una etapa 410, el TEDC determina un estado de suscripción de anclaje a red del dispositivo Android utilizando el archivo de configuración. El archivo de configuración generalmente incluye el estado de la suscripción de anclaje a red.

10 En una etapa 415, basado en al menos la determinación, se evita o bloquea el anclaje a red para impedir que el usuario use el dispositivo Android como medio para anclar a red el ordenador para acceder a Internet sin tener el contrato de servicio adecuado con el proveedor de servicios inalámbricos. Después de la etapa 420, el método 400 finaliza.

15 La figura 5 ilustra un método de refuerzo de anclaje a red 500 a modo de ejemplo detallado de acuerdo con la presente invención. El método 500 se produce después de que el dispositivo Android envía los datos preliminares al servidor. Como se explicó anteriormente, los datos preliminares generalmente incluyen información de identificación del dispositivo Android. En algunas realizaciones, el método 500 se produce después de que el dispositivo Android está acoplado al ordenador.

20 El método 500 se inicia en la etapa 505, en la que se determina si existe un archivo de configuración personalizado en el dispositivo Android. En algunas realizaciones, existe un archivo de configuración solo si el archivo de configuración se considera un archivo de configuración reciente. Por ejemplo, un archivo de configuración puede considerarse obsoleto y, por lo tanto, "inexistente" incluso si el archivo de configuración se ha descargado del servidor un día anterior o una hora antes. Incluso un archivo de configuración descargado recientemente puede estar desactualizado porque una nueva aplicación de anclaje a red de terceros podría haberse agregado al mercado desde que se descargó el archivo de configuración, el usuario podría haber agregado un plan de servicio de anclaje a red, o
25 ambos. En algunas realizaciones, cada archivo de configuración tiene una fecha/hora de vencimiento, después de lo cual el archivo de configuración caducó y se considera obsoleto.

30 Si se determina que el archivo de configuración no "existe" en la etapa 505, entonces, en una etapa 510, el archivo de configuración se descarga del servidor al dispositivo Android. Alternativamente, la etapa 510 siempre se realiza después de que el ordenador está conectado con el dispositivo Android. En algunas realizaciones, un archivo de configuración más reciente anula un archivo de configuración más antiguo.

35 Si se determina que el archivo de configuración existe en la etapa 505, entonces se determina si se ha lanzado una aplicación de anclaje a red. El usuario puede iniciar una aplicación de anclaje a red nativa o una aplicación de anclaje a red de terceros. Como tal, el TEDC escucha constantemente las transmisiones enviadas por el sistema Android para determinar si se ha lanzado una aplicación de anclaje a red nativa en la etapa 515a, mientras comprueba periódicamente el archivo de configuración con todas las aplicaciones en ejecución en el dispositivo Android para determinar si se ha iniciado una aplicación de terceros en la etapa 515b. Si hay una "coincidencia" en la etapa 515b, entonces se determina que se ha lanzado una aplicación de anclaje a red de terceros. Si se determina que no se inicia
40 ninguna aplicación de enlace en la etapa 515b, entonces, en una etapa 520, el TEDC espera una cantidad de tiempo predeterminada, como 10 segundos, antes de volver a la etapa 515. En algunas realizaciones, las etapas 505 y 510 ocurren después de las etapas 515 y 520.

45 Al determinar que una aplicación de anclaje a red, ya sea una aplicación de anclaje a red nativa o una aplicación de anclaje a red de terceros, ha sido lanzada en una etapa 525, se determina si existe un plan de servicio de anclaje a red basado en el archivo de configuración del usuario. Si el usuario no está suscrito a un plan de servicio de anclaje a red, luego, en la etapa 530, el TEDC desconecta o deshabilita el anclaje a red para evitar que el usuario use el dispositivo Android como medio para atar el ordenador para acceder a Internet sin tener el contrato de servicio adecuado con el proveedor de servicios inalámbricos. El TEDC puede solicitar al usuario uno o más mensajes. El
50 método 500 termina después de la etapa 530.

55 Sin embargo, si el usuario está suscrito a un plan de servicio de anclaje a red, luego, en la etapa 535, se permite el anclaje a red y el usuario puede continuar con el anclaje a red. En algunas realizaciones, si el usuario está bajo un período de prueba, se considera que el usuario está suscrito a un plan de servicio de anclaje a red. El TEDC puede solicitar al usuario uno o más mensajes. El método 500 se inicia en la etapa 535.

Controlador de dispositivo de refuerzo de anclaje a red de terceros

60 Supongamos que el usuario ha descargado una aplicación de anclaje a red de terceros, como una aplicación de anclaje a red de Bluetooth de terceros, una aplicación de enlace USB de terceros o una aplicación de anclaje a red genérico de terceros, para anclar a red el ordenador con el dispositivo Android. En algunas realizaciones, el TEDC puede detectar y bloquear el anclaje a red por completo de todas las aplicaciones de anclaje a red de terceros utilizadas para conectar el dispositivo Android con el ordenador. Cuando el usuario conecta el dispositivo Android con el ordenador, el TEDC enumerará todos los paquetes en ejecución en el dispositivo Android, utilizando la API
65 "Administrador de Actividad" en Android. El servidor asociado al proveedor inalámbrico mantiene una lista actualizada de los nombres de los paquetes de aplicaciones de anclaje a red. Esta información generalmente se descarga como

parte del archivo de configuración en el dispositivo Android cuando el usuario inicia el dispositivo Android, intenta anclar a red el dispositivo Android con el ordenador, o ambos.

5 Después de descargar el archivo de configuración, el TEDC compara la lista de paquetes en ejecución en el dispositivo Android con los valores en el archivo de configuración. Si la lista de paquetes en ejecución contiene alguno de los valores del paquete en el archivo de configuración, entonces el TEDC confirma que el usuario está intentando anclar a red. El TEDC intervendrá entonces y evitará el anclaje a red.

10 **Anclaje a red de Bluetooth de terceros.** En algunas realizaciones, cuando el usuario conecta el dispositivo Android con el ordenador con Bluetooth, el sistema Android lanzará la siguiente transmisión: "Android.bluetooth.device.action.ACL_CONNECTED". Una vez que el TEDC recibe esta transmisión, TEDC genera una lista de los paquetes que se ejecutan actualmente en el dispositivo Android. Una vez que se genera la lista de paquetes en ejecución, el TEDC comparará los paquetes en ejecución con los nombres de paquetes de aplicaciones en la lista negra. La lista de paquetes en ejecución se actualiza periódicamente. Si una aplicación de anclaje a red de
15 terceros, como PDANet, está habilitado o lanzado, entonces la aplicación PDANet se incluirá en la lista. Si hay aplicaciones en la lista negra ejecutándose, entonces el TEDC evita el anclaje a red según el estado de suscripción del servicio de anclaje a red del usuario.

20 En algunas realizaciones, durante un período de prueba, el usuario podrá conectarse pero se le informará sobre el estado de la suscripción de prueba. La figura 6A ilustra una notificación a modo de ejemplo mostrada durante el período de prueba de acuerdo con la presente invención. En algunas realizaciones, después del período de prueba, si el usuario no se suscribe a un plan de anclaje a red, en cada intento de anclaje a red posterior, el TEDC desconectará el anclaje a red Bluetooth deshabilitando la marca de anclaje a red de Bluetooth para bloquear el anclaje a red, con o sin notificación personalizada. La figura 6B ilustra una notificación a modo de ejemplo mostrada bajo la categoría
25 bloqueada de acuerdo con la presente invención. En algunas realizaciones, si el usuario se suscribe o está suscrito a un plan de anclaje a red, entonces el TEDC no bloqueará el anclaje a red, con o sin notificación personalizada.

30 **Anclaje a red de USB de terceros.** En algunas realizaciones, cuando el usuario conecta el dispositivo Android con el ordenador con USB, el sistema Android lanzará las siguientes transmisiones: "Android.net.conn.TETHER_STATE_CHANGED", "Android.intent.action.ACTION_POWER_CONNECTED", y "android.intent.action.UMS_CONNECTED". Según una permutación de estas transmisiones o intentos, el TEDC validará el anclaje a red del ordenador si la diferencia entre las marcas de tiempo de los intentos es menor que una cantidad de tiempo predeterminada, como 1500 milisegundos. Tras una determinación de conexión USB, TEDC genera una lista de los paquetes que se ejecutan actualmente en el dispositivo Android. Una vez que se genera la lista
35 de paquetes en ejecución, el TEDC comparará los paquetes en ejecución con los nombres de paquetes de aplicaciones en la lista negra. La lista de paquetes en ejecución se actualiza periódicamente. Si una aplicación de anclaje a red de terceros, como PDANet, está habilitado o lanzado, entonces la aplicación PDANet se incluirá en la lista. Si hay aplicaciones en la lista negra ejecutándose, entonces el TEDC evita el anclaje a red según el estado de suscripción del servicio de anclaje a red del usuario.

40 En algunas realizaciones, durante un período de prueba, el usuario podrá conectarse pero se le informará sobre el estado de la suscripción de prueba. (Ver la figura 6A). En algunas realizaciones, después del período de prueba, si el usuario no se suscribe a un plan de anclaje a red, en cada intento de anclaje a red posterior, el TEDC desconectará la conexión USB deshabilitando la marca de depuración USB y la marca de anclaje a red USB para bloquear el anclaje a red, con o sin notificación personalizada. (Ver la figura 6B). En algunas realizaciones, si el usuario se suscribe o está suscrito a un plan de anclaje a red, entonces el TEDC no bloqueará el anclaje a red, con o sin notificación
45 personalizada.

50 *Controlador de dispositivo de aplicación de anclaje a red nativa*

Ahora, supongamos que el usuario habilita el anclaje a red nativa, como el anclaje a red Bluetooth nativa, anclaje a red USB nativa o Wi-Fi portátil para anclar a red el ordenador con el dispositivo Android. Ahora se discutirá cada uno de estos escenarios.

55 **Controlador de aplicación de anclaje a red Bluetooth nativa.** En algunas realizaciones, cuando el usuario intenta conectar Internet móvil habilitando el anclaje a red Bluetooth nativa, el sistema Android lanzará las siguientes transmisiones: "Android.bluetooth.device.action.ACL_CONNECTED", "Android.bluetooth.pan.profile.action.CONNECTION_STATE_CHANGED",
60 "Android.bluetooth.intent.action.BLUETOOTH_STATE_CHANGED". El TEDC está configurado para monitorear estas transmisiones. En algunas realizaciones, el TEDC verificará el anclaje a red con el intento "android.bluetooth.pan.profile.action.CONNECTED". El TEDC también mirará el archivo de configuración. Si el archivo de configuración no existe, entonces el TEDC descargará el archivo de configuración. El TEDC compara el estado de suscripción del usuario. Si el usuario está bajo un período de prueba, el usuario podrá anclarse a red pero se le informará sobre el estado de suscripción del usuario. Si el usuario está en la categoría bloqueada, entonces el TEDC
65 bloqueará el anclaje a red desactivando la marca de anclaje a red Bluetooth, con o sin notificación personalizada. Esta anclaje a red Bluetooth está desactivada sin interrumpir ninguna otra conexión Bluetooth, como auriculares o una ruta

de audio. Si el usuario está bajo la categoría permitida, entonces el TEDC no bloqueará el anclaje a red, con o sin notificación personalizada.

5 **Controlador de aplicación de anclaje a red USB nativa.** En algunas realizaciones, cuando el usuario intenta conectar Internet móvil habilitando el anclaje a red USB nativa, el sistema Android lanzará la siguiente transmisión: "Android.net.conn.TETHER_STATE_CHANGE". El TEDC monitorea la transmisión. En algunas realizaciones, el TEDC verificará el anclaje a red USB mediante la API de Java Reflection o similar. En algunas realizaciones, La anclaje a red USB se valida cuando la cadena devuelta contiene el valor "usb01" o el valor "mdis". El TEDC también mirará el archivo de configuración. Si el archivo de configuración no existe, entonces el TEDC descargará el archivo de configuración. Si el archivo de configuración no existe, entonces el TEDC descargará el archivo de configuración. El TEDC compara el estado de suscripción del usuario. Si el usuario está bajo un período de prueba, el usuario podrá anclarse a red pero se le informará sobre el estado de suscripción del usuario. Si el usuario está en la categoría bloqueada, entonces el TEDC bloqueará el anclaje a red desactivando la marca de depuración USB y la marca de anclaje a red USB, con o sin notificación personalizada. Si el usuario está bajo la categoría permitida, entonces el TEDC no bloqueará el anclaje a red, con o sin notificación personalizada.

15 **Controlador de dispositivo de aplicación de anclaje a red de punto de acceso Wi-Fi portátil.** En algunas realizaciones, cuando el usuario intenta anclar a red Internet móvil habilitando el punto de acceso Wi-Fi portátil, el sistema Android lanzará la siguiente transmisión: "Android.net.conn.TETHER_STATE_CHANGE". El TEDC escucha la transmisión. En algunas realizaciones, el TEDC verificará el anclaje a red de puntos de acceso Wi-Fi mediante la API de Java Reflection o similar. En algunas realizaciones, El anclaje a red de la zona Wi-Fi se valida cuando la cadena devuelta contiene el valor "w". El TEDC también mirará el archivo de configuración. Si el archivo de configuración no existe, entonces el TEDC descargará el archivo de configuración. El TEDC compara el estado de suscripción del usuario. Si el usuario está bajo un período de prueba, el usuario podrá anclarse a red pero se le informará sobre el estado de suscripción del usuario. Si el usuario está en la categoría bloqueada, entonces el TEDC bloqueará el anclaje a red al deshabilitar la marca de punto de acceso Wi-Fi, con o sin notificación personalizada. Si el usuario está bajo la categoría permitida, entonces el TEDC no bloqueará el anclaje a red, con o sin notificación personalizada.

Ventajas

30 Un proveedor de servicios inalámbricos puede enviar un archivo de configuración, en formato XML u otro formato adecuado, desde el servidor del proveedor de servicios inalámbricos al dispositivo de un usuario en cada intento de anclaje a red por parte de un usuario. Este archivo XML contiene valores de nombres de paquetes de aplicaciones en la lista negra, estado de suscripción del usuario (por ejemplo, prueba, bloqueado o permitido) y cualquier mensaje de solicitud personalizado que se muestre en el dispositivo del usuario.

35 El TEDC permite ventajosamente a los proveedores de servicios inalámbricos informar a los usuarios sobre el anclaje a red mediante notificaciones personalizadas. En algunas realizaciones, los proveedores de servicios inalámbricos pueden notificar a los usuarios cuando los usuarios con CTN móviles únicos e IMEI del dispositivo intentan anclarse a red. En algunas realizaciones, las notificaciones personalizadas incluyen la tasa de uso de datos para el ciclo de facturación actual y otra información útil sobre los servicios de datos suscritos, servicios de anclaje a red o ambos.

40 El TEDC asegura ventajosamente que el uso de los servicios de anclaje a red sea apropiado y deshabilita el anclaje a red incorrecto. En algunas realizaciones, el TEDC monitorea y controla eficientemente el anclaje a red con ciclos mínimos de CPU y batería.

45 El TEDC ayuda ventajosamente a los operadores inalámbricos a alertar y obtener/mantener el control del uso de datos móviles para, de ese modo, preservar y controlar el ancho de banda móvil.

50 Debe entenderse que, si bien la invención se ha descrito en relación con implementaciones específicas para el sistema operativo Android, se pueden realizar implementaciones similares para otros dispositivos inteligentes que ejecutan otros sistemas operativos.

55 Si bien la invención se ha descrito con referencia a numerosos detalles específicos, un experto en la materia reconocerá que la invención puede realizarse de otras formas específicas. Por lo tanto, un experto en la materia entenderá que la invención no está limitada por los detalles ilustrativos anteriores, sino que se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema (300), que comprende:

- 5 a. un segundo dispositivo (310), que incluye una memoria no transitoria; y
- b. un primer dispositivo (305), que incluye una memoria no transitoria para almacenar instrucciones, las instrucciones para:
 - 10 1. acceder a un archivo de configuración personalizado desde un servidor al primer dispositivo;
 - 2. determinar el estado de suscripción de anclaje a red del primer dispositivo, en donde la determinación se basa en el archivo de configuración personalizado;
 - 15 3. escuchar las transmisiones enviadas por el primer dispositivo para determinar si se ha lanzado una aplicación de anclaje a red nativa del primer dispositivo, según el estado de la suscripción de anclaje a red, bloquear el segundo dispositivo para que no se ancle a red con el primer dispositivo si se ha lanzado una aplicación de anclaje a red nativa del primer dispositivo;

comparar periódicamente el archivo de configuración personalizado con las aplicaciones en ejecución en el primer dispositivo, para determinar si se ha iniciado una aplicación de anclaje a red de terceros; en donde dicha comparación comprende comparar una lista de aplicaciones en ejecución en el primer dispositivo con valores de paquete de aplicaciones de anclaje a red de terceros en el archivo de configuración personalizado, y si la lista de aplicaciones en ejecución contiene cualquiera de los valores de paquete de aplicaciones de anclaje a red de terceros en el archivo de configuración, impedir el anclaje a red.

2. El sistema de la reivindicación 1, en el que el archivo de configuración personalizado se basa en servicios de suscripción de anclaje a red, e incluye nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros.

3. El sistema de la reivindicación 1, en el que las instrucciones también son para presentar un mensaje sobre el estado de la suscripción de anclaje a red.

4. El sistema de la reivindicación 1, en el que las instrucciones también son para enviar datos preliminares al servidor, en donde los datos preliminares incluyen información de identificación del primer dispositivo.

5. El sistema de la reivindicación 1, en el que las instrucciones también son para determinar todas las aplicaciones actualmente activas, que se ejecutan en el primer dispositivo.

6. El sistema de la reivindicación 1, en el que las instrucciones se invocan al arrancar el sistema operativo del aparato o al anclar a red el primer dispositivo con el otro dispositivo.

7. Un medio legible por ordenador no transitorio, que almacena instrucciones que, cuando son ejecutadas por un dispositivo informático (305), hacen que el dispositivo informático (305) lleve a cabo un método, que comprende:

- a. enviar información de identificación del dispositivo informático (305) a un servidor (315);
- b. recibir del servidor (315) un archivo de configuración personalizado basado en la información de identificación;
- 45 c. determinar si se ha evocado una aplicación de anclaje a red en el dispositivo informático (305); en donde determinar comprende escuchar transmisiones enviadas por el dispositivo informático para determinar si se ha lanzado una aplicación de anclaje a red nativa del dispositivo informático; y en donde la determinación comprende además comparar periódicamente el archivo de configuración personalizado con las aplicaciones en ejecución en el dispositivo informático, para determinar si se ha lanzado una aplicación de anclaje a red de terceros;
- 50 d. basado en dicha determinación de verificación de la permisibilidad de anclaje a red de un dispositivo de anclaje a red (310) con el dispositivo informático (305), basado en el archivo de configuración personalizado; y
- e. desconectar el anclaje a red del dispositivo de anclaje a red (310) del dispositivo informático (305), cuando el anclaje a red no está permitido, y permitir el anclaje a red del dispositivo de anclaje a red (310) con el dispositivo informático (305), cuando el anclaje a red está permitido.

8. El medio legible por ordenador no transitorio de la reivindicación 7, en el que, cuando la aplicación de anclaje a red es una aplicación de anclaje a red de terceros, determinar si se ha evocado una aplicación de anclaje a red comprende:

- a. escuchar una o más transmisiones por el dispositivo informático;
- 60 b. generar una lista de paquetes actualmente en ejecución en el dispositivo informático; y
- c. comparar la lista de paquetes actualmente en ejecución con una lista de nombres de paquetes de aplicaciones actualmente incluidos en la lista negra incluidos en el archivo de configuración.

9. El medio legible por ordenador no transitorio de la reivindicación 7, en el que, cuando la aplicación de anclaje a red es una aplicación de anclaje a red nativa, determinar si se ha evocado una aplicación de anclaje a red, comprende:

- a. escuchar una o más transmisiones por el dispositivo informático; y
- b. validar el anclaje a red del dispositivo de anclaje a red con el dispositivo informático.

5 10. El medio legible por ordenador no transitorio de la reivindicación 7, en el que la verificación de la permisibilidad del anclaje a red incluye hacer referencia al archivo de configuración personalizado.

11. Un sistema de anclaje a red (300), que comprende:

- 10 a. una red (320);
- b. un servidor (315), acoplado comunicativamente con la red (320), en donde el servidor (315) incluye perfiles de clientes y nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros, y en donde el servidor (315) está configurado para generar archivos de configuración personalizados; y
- 15 c. un dispositivo primario (305), acoplado comunicativamente con la red (320), en donde el dispositivo primario (305) está configurado para:

- 1. proporcionar información de identificación del dispositivo primario (305) al servidor (315);
- 2. descargar un archivo de configuración personalizado del servidor (315), en donde el archivo de configuración personalizado es generado por el servidor (315) de acuerdo con la información de identificación; y
- 20 3. basado en al menos el archivo de configuración personalizado, realizar uno de no permitir y permitir el anclaje a red de un dispositivo secundario (310) con el dispositivo primario (305), al detectar el anclaje a red, en donde la detección comprende escuchar transmisiones enviadas por el dispositivo primario para determinar si se ha lanzado una aplicación de anclaje a red nativa del dispositivo primario; y en donde la detección comprende además comparar periódicamente el archivo de configuración personalizado con las aplicaciones en ejecución
- 25 en el dispositivo primario para determinar si se ha lanzado una aplicación de enlace de terceros.

12. El sistema de anclaje a red de la reivindicación 11, en el que el archivo de configuración personalizado incluye perfiles de clientes y nombres de paquetes actualmente en la lista negra de aplicaciones de anclaje a red de terceros, y en donde cada perfil de cliente incluye información de suscripción de anclaje a red relacionado con un cliente.

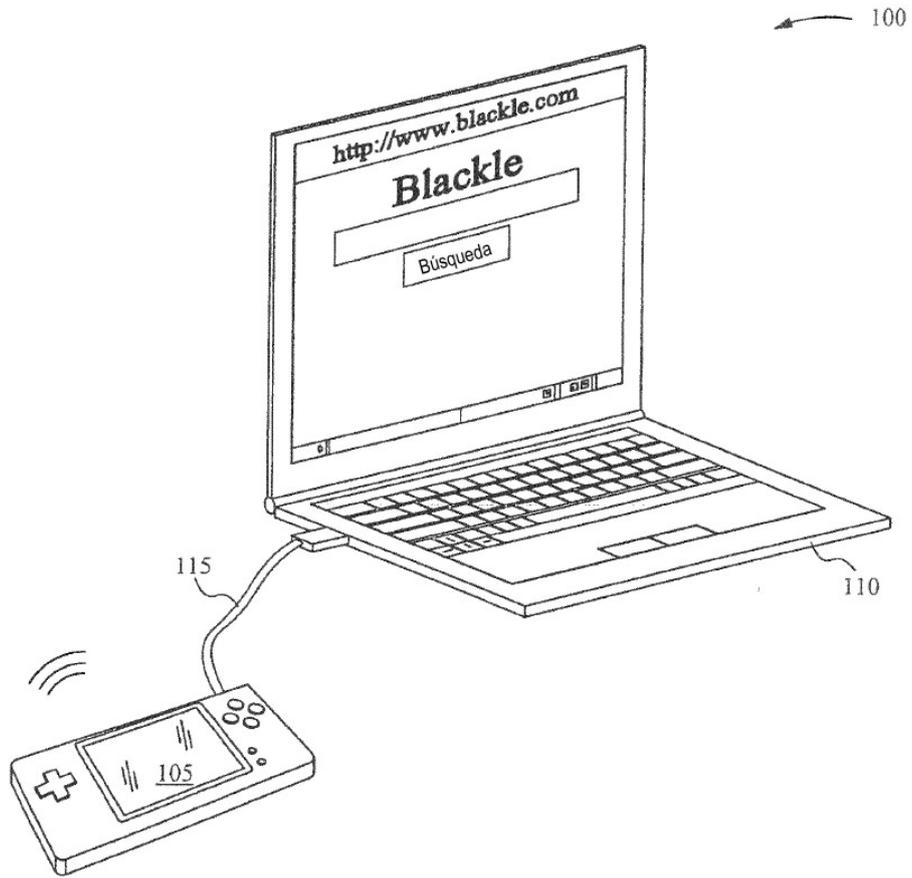


Fig. 1

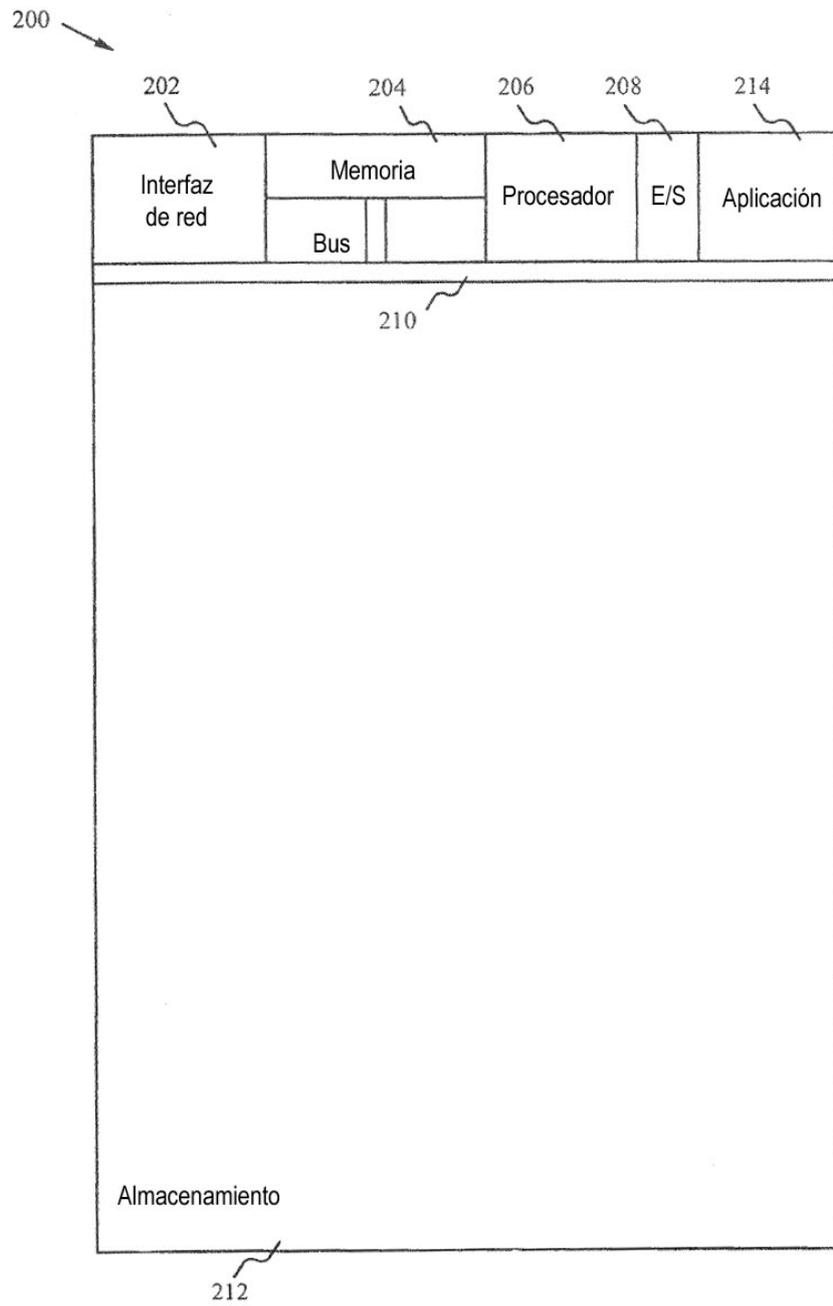


Fig. 2

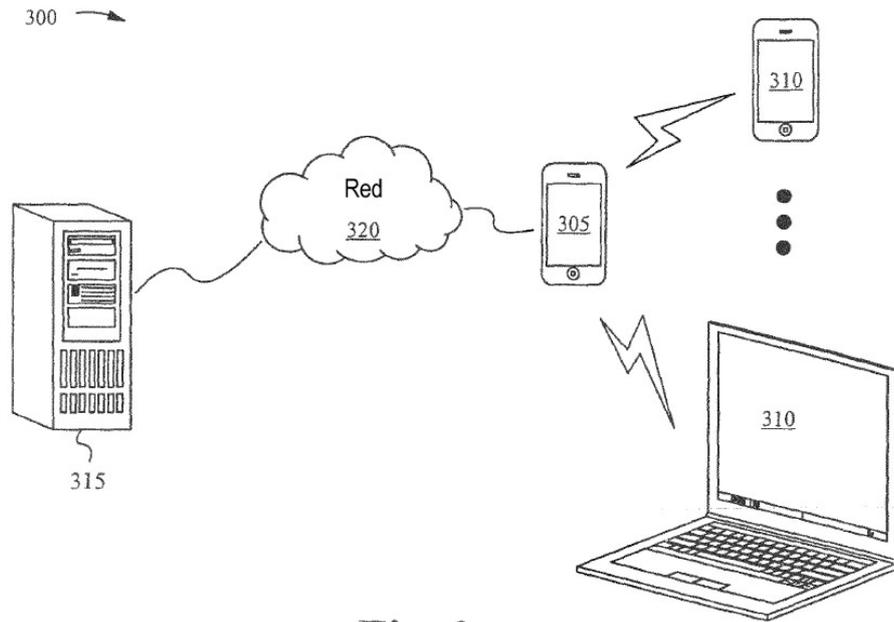


Fig. 3

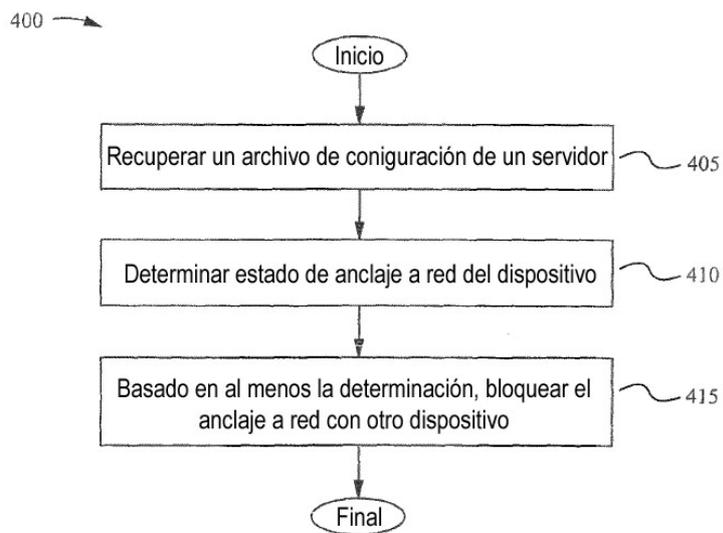


Fig. 4

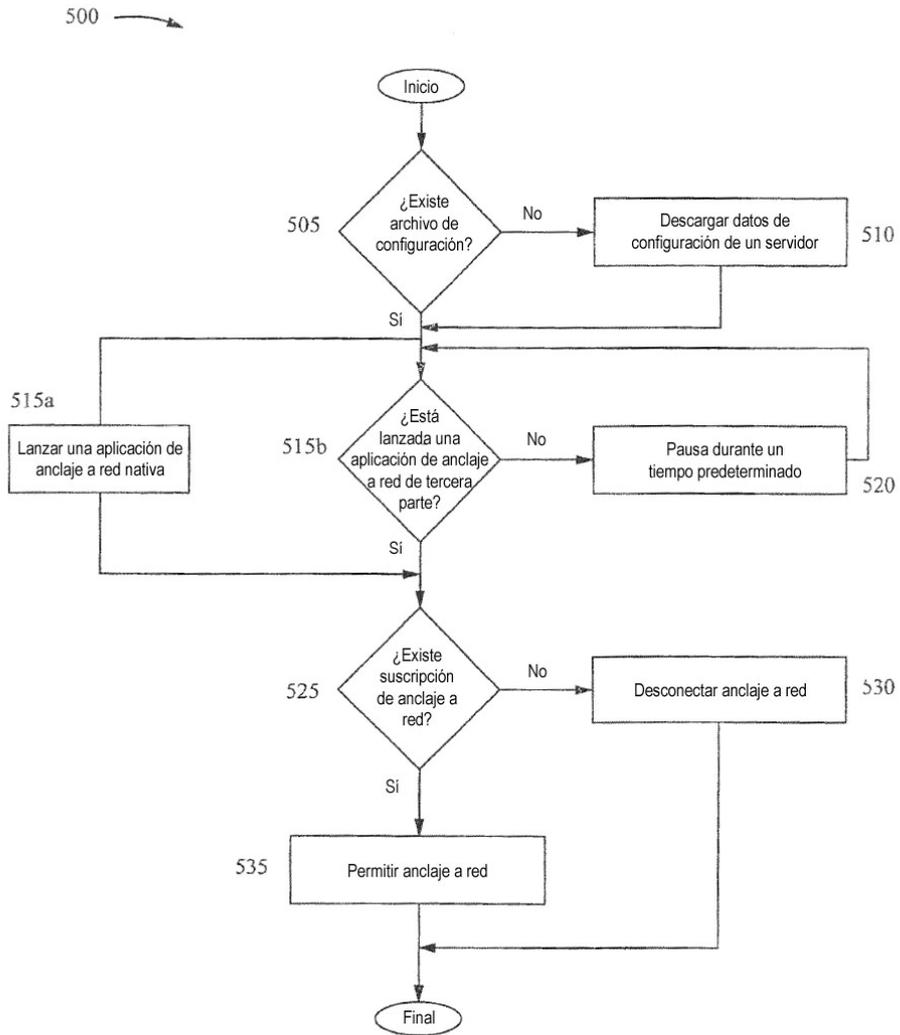


Fig. 5

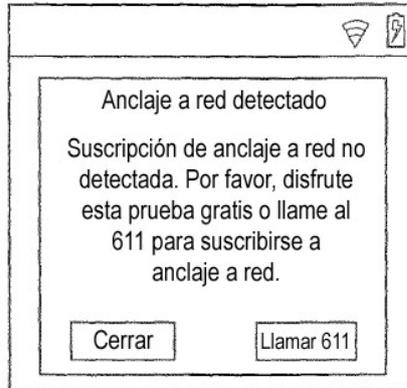


Fig. 6A

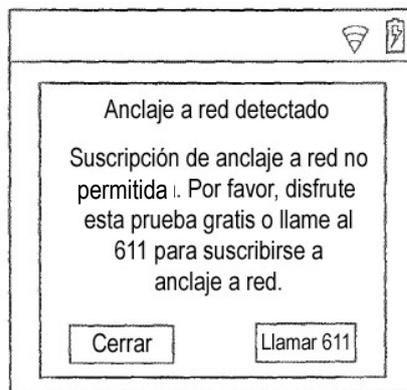


Fig. 6B