(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 656 141**

(51) Int. Cl.:

H04W 12/06 (2009.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 84/12 (2009.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.06.2012** **PCT/FI2012/050577**

(87) Fecha y número de publicación internacional: **14.02.2013** **WO13021094**

(96) Fecha de presentación y número de la solicitud europea: **08.06.2012** **E 12821728 (8)**

(97) Fecha y número de publicación de la concesión europea: **01.11.2017** **EP 2740315**

(54) Título: **Método, aparato y producto de programa informático para la configuración de conexión en una comunicación de dispositivo a dispositivo**

(30) Prioridad:

05.08.2011 US 201113198984

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.02.2018

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

SUUMÄKI, JAN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 656 141 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

Método, aparato y producto de programa informático para la configuración de conexión en una comunicación de dispositivo a dispositivo

Campo:

El campo de la invención se refiere a la comunicación inalámbrica y, más en particular, a la configuración de conexión en una comunicación de dispositivo a dispositivo usando una portadora fuera de banda.

Antecedentes:

La sociedad moderna ha adoptado, y está empezando a depender de, dispositivos de comunicación inalámbrica para diversos fines, tales como conectar a los usuarios de los dispositivos de comunicación inalámbrica con otros usuarios. Los dispositivos de comunicación inalámbrica pueden variar de dispositivos de mano alimentados por baterías a dispositivos comerciales y/o electrodomésticos estacionarios que utilizan una red eléctrica como fuente de alimentación. Debido al rápido desarrollo de los dispositivos de comunicación inalámbrica, ha surgido un número de áreas que pueden posibilitar completamente nuevos tipos de aplicaciones de comunicación.

Las redes celulares facilitan la comunicación a través de grandes áreas geográficas. Estas tecnologías de red se han dividido comúnmente por generaciones, comenzando a finales de la década de 1970 a principios de la década de 1980 con los teléfonos celulares analógicos de primera generación (1G) que proporcionaban comunicaciones de voz básicas, a los modernos teléfonos celulares digitales. GSM es un ejemplo de una red celular digital 2G ampliamente empleada que se comunica en las bandas de 900 MHz/1,8 GHz en Europa y a 850 MHz y 1,9 GHz en los Estados Unidos. A pesar de que las redes de comunicación de largo alcance, como GSM, son un medio bien aceptado para transmitir y recibir datos, debido al coste, el tráfico y cuestiones legislativas, puede que estas redes no sean apropiadas para todas las aplicaciones de datos.

Las tecnologías de comunicación de corto alcance proporcionan soluciones de comunicación que evitan algunos de los problemas observados en las redes celulares grandes. Bluetooth™ es un ejemplo de una tecnología inalámbrica de corto alcance que está obteniendo rápidamente aceptación en el mercado. Además de Bluetooth™, otras tecnologías populares de comunicación de corto alcance incluyen las tecnologías de Baja Energía de Bluetooth™, red de área local inalámbrica (WLAN) de IEEE 802.11, USB inalámbrico (WUSB), banda ultraancha (UWB), ZigBee (IEEE 802.15.4, IEEE 802.15.4a) e identificación por radiofrecuencia de ultra alta frecuencia (RFID de UHF). La totalidad de estas tecnologías de comunicación inalámbrica presentan características y ventajas que las hacen apropiadas para diversas aplicaciones.

Las tecnologías de comunicación de campo cercano, tales como las tecnologías de identificación por radiofrecuencia (RFID), comprenden una gama de sistemas de transmisión por RF, por ejemplo, sistemas normalizados y patentados para un gran número de fines diferentes, tales como el etiquetado de productos para gestión de inventario y logística, fines de evitación de robos en el punto de venta y reciclaje de productos al final del ciclo de vida del producto etiquetado. Además de las tecnologías de RFID, la tecnología de comunicación de campo cercano (NFC) ha evolucionado recientemente a partir de una combinación de las tecnologías de identificación y de interconexión sin contacto existentes. NFC es una tecnología tanto de "lectura" como de "escritura". la comunicación entre dos dispositivos compatibles con NFC tiene lugar cuando estos se ponen muy próximos uno de otro: Una simple onda o toque puede establecer una conexión de NFC que se puede usar para intercambiar una información específica para otro protocolo de comunicaciones, que se puede usar entonces para crear una conexión real en el otro protocolo de comunicaciones, tal como Bluetooth™ o red de área local inalámbrica (WLAN).

El documento USB2004/103312 divulga un sistema de gestión de derechos digitales basado en dominio en el que se añaden nuevos dispositivos a un dominio existente mediante la obtención de una información de dominio (por ejemplo, un nombre de dominio y una contraseña de dominio privada) desde dispositivos ya en el dominio que, preferentemente, se encuentran muy próximos. Una vez que la información de dominio se ha transferido desde el dispositivo ya en el dominio al dispositivo que se está añadiendo al dominio, el dispositivo que se está añadiendo al dominio entra en contacto con un emisor de claves para completar su registro en el dominio. El emisor de claves devuelve una clave privada de dominio de DRM así como un certificado de DRM. Ambos son utilizados por el dispositivo para obtener y representar contenido digital.

El documento WO2006/106393 divulga métodos y sistemas para gestionar el acceso a una red de área local inalámbrica. Un punto de acceso inalámbrico (AP) puede usar un enfoque unificado que utiliza un canal fuera de banda para comunicar información de claves de autenticación y de dirección de red a un dispositivo de invitado, y utiliza un canal dentro de banda para establecer comunicaciones con el dispositivo de invitado, y también proporciona soporte para la configuración dentro de banda en todos los dispositivos. La capacidad de usar fuera de banda donde sea posible prevé un aumento para la seguridad y la facilidad de uso, y la posibilidad de delegar el acceso de un dispositivo a otro. Por lo tanto, el enfoque unificado también proporciona una gestión sencilla del acceso de invitado a la WLAN.

El documento USB2009/264098 divulga un sistema y método para configurar dispositivos para la comunicación inalámbrica. Un método puede incluir transmitir una clave de activación desde un intermediario de activación a un agente inalámbrico. El método también puede incluir transmitir la clave de activación desde el intermediario de activación a un registrador inalámbrico. Al menos una de la transmisión de la clave de activación al agente inalámbrico y la transmisión de la clave de activación al registrador inalámbrico puede incluir transmitir la clave de activación por medio de una tecnología de comunicación inalámbrica de corto alcance. Además, la clave de activación puede incluir información para autenticar la comunicación inalámbrica entre el agente inalámbrico y un punto de acceso inalámbrico.

Sumario

Se divulgan realizaciones de método, de aparato y de producto de programa informático para posibilitar la configuración de conexión en una comunicación de dispositivo a dispositivo usando portadora fuera de banda. Algunas realizaciones a modo de ejemplo de la invención incluyen un método que comprende:

participar, por parte de un primer dispositivo, en una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo;

intercambiar, por parte del primer dispositivo, información con un segundo dispositivo que no está conectado con la red inalámbrica, a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo el intercambio de información:

recibir, desde el segundo dispositivo, una información de autenticación por medio de una portadora de corto alcance fuera de banda inalámbrica, para su reenvío al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

enviar, al segundo dispositivo, unos parámetros de conexión de comunicación dentro de banda por medio de la portadora de corto alcance fuera de banda inalámbrica, para la conexión a la red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

transmitir, la información de autenticación recibida, al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo, por medio de la conexión de comunicación de portadora de corto alcance dentro de banda.

Algunas realizaciones a modo de ejemplo de la invención incluyen un método que comprende:

intercambiar, por parte de un segundo dispositivo que no está conectado a una red inalámbrica, información con un primer dispositivo, a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo la información intercambiada:

transmitir, por parte del segundo dispositivo, una información de autenticación reconocible por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica; y

recibir, por parte del segundo dispositivo, unos parámetros de conexión de comunicación dentro de banda para habilitar al aparato para la conexión a la red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

transmitir, por parte del segundo dispositivo, la información de autenticación al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo por medio de una conexión de comunicación dentro de banda para posibilitar que el aparato se una a la red inalámbrica, de acuerdo con los parámetros de conexión de comunicación dentro de banda.

Algunas realizaciones a modo de ejemplo de la invención incluyen un método que comprende:

recibir, por parte de un dispositivo de punto de acceso o un dispositivo de propietario de grupo, una primera información de autenticación desde un primer dispositivo inalámbrico conectado a una red inalámbrica por medio de una conexión de comunicación dentro de banda;

recibir, por parte del dispositivo de punto de acceso o el dispositivo de propietario de grupo, una segunda información de autenticación, desde el segundo dispositivo inalámbrico, por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda; y

conceder, por parte del dispositivo de punto de acceso o el dispositivo de propietario de grupo, acceso al segundo dispositivo para unirse a la red inalámbrica por medio de la segunda conexión de comunicación dentro de banda, si se corresponden la primera y la segunda información de autenticación recibidas.

Algunas realizaciones a modo de ejemplo de la invención incluyen un programa informático que comprende código de programa legible por ordenador configurado para dar lugar a la realización del método de cualquiera de las realizaciones anteriores a modo de ejemplo de la invención. Algunas realizaciones a modo de ejemplo de la invención incluyen un aparato que comprende:

unos medios para participar en una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo;
unos medios para intercambiar información con un segundo dispositivo que no está conectado a la red inalámbrica a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo los medios para intercambiar información:

unos medios para recibir, desde el segundo dispositivo, una información de autenticación por medio de una portadora de corto alcance fuera de banda inalámbrica para su reenvío al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo;

unos medios para enviar, al segundo dispositivo, unos parámetros de conexión de comunicación dentro de banda por medio de la portadora de corto alcance fuera de banda inalámbrica, para la conexión a la red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

unos medios para transmitir, la información de autenticación recibida, al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo, por medio de la conexión de comunicación de portadora de corto alcance dentro de banda.

Algunas realizaciones a modo de ejemplo de la invención incluyen un aparato que comprende:

unos medios para intercambiar información con un primer dispositivo a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo los medios para intercambiar información:

unos medios para transmitir una información de autenticación reconocible por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica; y

unos medios para recibir unos parámetros de conexión de comunicación dentro de banda para posibilitar que el aparato se conecte con una red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

unos medios para transmitir la información de autenticación al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo por medio de una conexión de comunicación dentro de banda, de acuerdo con los parámetros de conexión de comunicación dentro de banda.

Algunas realizaciones a modo de ejemplo de la invención incluyen un dispositivo de punto de acceso o un aparato de propietario de grupo para una red inalámbrica, que comprende:

unos medios para recibir una primera información de autenticación, desde un primer dispositivo inalámbrico conectado a una red inalámbrica por medio de una conexión de comunicación dentro de banda;

unos medios para recibir una segunda información de autenticación, desde un segundo dispositivo inalámbrico, por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda; y

unos medios para conceder acceso al segundo dispositivo para unirse a la red inalámbrica por medio de la segunda conexión de comunicación dentro de banda, si se corresponden la primera y la segunda información de autenticación recibidas.

Las realizaciones resultantes posibilitan una conmutación de transporte de portadora de comunicación de corto alcance fuera de banda para la configuración de conexión en una comunicación de dispositivo a dispositivo con un dispositivo de punto de acceso o un dispositivo de propietario de grupo.

Descripción de las figuras:

La figura 1A ilustra un diagrama de red a modo de ejemplo antes de que se hayan conectado los nodos, en el que el dispositivo A, el dispositivo B y el AP/GO de dispositivo central incluyen un transceptor de portadora de corto alcance dentro de banda, tal como un transceptor de WLAN de IEEE 802.11. El dispositivo A y el dispositivo B incluyen adicionalmente un transceptor de portadora de corto alcance fuera de banda, tal como un transceptor de comunicación de campo cercano (NFC), de acuerdo con algunas realizaciones a modo de ejemplo de la invención.
La figura 1B ilustra el diagrama de red a modo de ejemplo de la figura 1A, en el que el dispositivo A se muestra

como habiéndose unido a una red WLAN al haber formado una conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 con el AP/GO de dispositivo central, representando el AP/GO de dispositivo central o bien un dispositivo de punto de acceso (AP) en una red de infraestructura o bien un dispositivo de propietario de grupo (GO) en una red P2P, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1C ilustra el diagrama de red a modo de ejemplo de la figura 1B, en el que el AP/GO de dispositivo central se muestra transmitiendo una información de autenticación al dispositivo A por medio de la conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1D ilustra el diagrama de red a modo de ejemplo de la figura 1C, en el que se pone en práctica un evento de toque de NFC entre los dispositivos A y B con el fin de iniciar un procedimiento de conmutación de transporte de portadora de corto alcance con el dispositivo B, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1E ilustra el diagrama de red a modo de ejemplo de la figura 1D, de un ejemplo en el que el dispositivo B envía una solicitud de traspaso de NFC al dispositivo A, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1F ilustra el diagrama de red a modo de ejemplo de la figura 1E, de un ejemplo en el que el dispositivo A responde con una selección de traspaso de NFC que incluye la información de autenticación que es reconocible por el AP/GO de dispositivo central y una información de conexión, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1G ilustra el diagrama de red a modo de ejemplo de la figura 1F, en el que el dispositivo B envía una trama de solicitud, por ejemplo, una trama de solicitud de sondeo, con un elemento de información (IE) de configuración protegida de Wi-Fi (WSC) al AP/GO de dispositivo central en un procedimiento de configuración protegida de Wi-Fi. El elemento de información (IE) de WSC de incluye la información de autenticación reconocible por el AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1H ilustra el diagrama de red a modo de ejemplo de la figura 1G, en el que el AP/GO de dispositivo central reconoce la información de autenticación que sirve como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. El AP/GO de dispositivo central concede un acceso de red al dispositivo B y, después de una señalización adicional, envía credenciales al dispositivo B, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1I ilustra el diagrama de red a modo de ejemplo de la figura 1G, en el que el dispositivo B está ahora conectado a la red con su nueva configuración y se puede comunicar con el dispositivo A a través de la red, a través del AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 1J ilustra el diagrama de red a modo de ejemplo de la figura 1D, de un ejemplo alternativo en el que el dispositivo A transmite al dispositivo B una solicitud de traspaso de NFC que incluye la información de autenticación que es reconocible por el AP/GO de dispositivo central y una información de conexión, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 2 es un diagrama de bloques funcionales a modo de ejemplo del dispositivo A y el dispositivo B de la figura 1A, que muestra cada dispositivo equipado con un transceptor de NFC fuera de banda y un transceptor de portadora de corto alcance dentro de banda, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 3A es una realización a modo de ejemplo de un ejemplo de un mensaje de solicitud de traspaso de NFC desde el dispositivo B al dispositivo A con una solicitud de información para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 3B es una realización a modo de ejemplo de un ejemplo de un mensaje de selección de traspaso de NFC enviado desde el dispositivo A al dispositivo B para proporcionar ajustes de conectividad y la información de autenticación reconocible por el AP/GO de dispositivo central, para obtener un acceso de red a través del AP/GO de dispositivo central, de acuerdo con una realización de la presente invención.

La figura 3C es una realización alternativa a modo de ejemplo de un ejemplo de un mensaje de solicitud de traspaso de NFC enviado desde el dispositivo A al dispositivo B, tal como se muestra en la figura 1J, para proporcionar ajustes de conectividad y la información de autenticación reconocible por el AP/GO de dispositivo

central, para obtener un acceso de red a través del AP/GO de dispositivo central, de acuerdo con una realización de la presente invención.

La figura 4 es un diagrama de bloques funcionales a modo de ejemplo del dispositivo B y el AP/GO de dispositivo central de la figura 1A, en el que el dispositivo B envía la información de autenticación al AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A y, en respuesta, el AP/GO de dispositivo central envía unas credenciales de red al dispositivo B, de acuerdo con una realización de la presente invención.

La figura 5A ilustra una trama de solicitud de IEEE 802.11 a modo de ejemplo, por ejemplo, una trama de solicitud de sondeo enviada por el dispositivo B al AP/GO de dispositivo central con la información de autenticación en un elemento de información de WSC, de acuerdo con una realización de la presente invención.

La figura 5B ilustra una trama de gestión de MAC a modo de ejemplo enviada por el AP/GO de dispositivo central al dispositivo B con uno de los mensajes M2, M4, M6 y M8 en un elemento de información de WSC, que se usa para ensamblar las credenciales de red en el dispositivo B, de acuerdo con una realización de la presente invención.

La figura 6A es un diagrama de flujo a modo de ejemplo de etapas operativas de una realización a modo de ejemplo del método llevado a cabo por el dispositivo A de la figura 2, de acuerdo con una realización de la presente invención.

La figura 6B es un diagrama de flujo a modo de ejemplo de etapas operativas de una realización a modo de ejemplo del método llevado a cabo por el dispositivo B de la figura 2, de acuerdo con una realización de la presente invención.

La figura 6C es un diagrama de flujo a modo de ejemplo de etapas operativas de una realización a modo de ejemplo del método llevado a cabo por el AP/GO de dispositivo central de la figura 4, de acuerdo con una realización de la presente invención.

La figura 7 es un diagrama de secuencia a modo de ejemplo de una realización a modo de ejemplo que muestra la interacción del dispositivo A, el dispositivo B y el AP/GO de dispositivo central de la figura 1B, de acuerdo con una realización de la presente invención.

La figura 8A ilustra el diagrama de red a modo de ejemplo de la figura 1A, en el que el dispositivo A se muestra como habiéndose unido a una red WLAN al haber formado una conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 con el AP/GO de dispositivo central, y el dispositivo B se muestra habiendo generado la información de autenticación, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8B ilustra el diagrama de red a modo de ejemplo de la figura 8A, se pone en práctica un evento de toque de NFC entre los dispositivos A y B con el fin de iniciar un procedimiento de conmutación de transporte de portadora de corto alcance con el dispositivo B, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8C ilustra el diagrama de red a modo de ejemplo de la figura 8B, un ejemplo en el que el dispositivo B está enviando una solicitud de traspaso de NFC al dispositivo A que incluye una información de autenticación, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8D ilustra el diagrama de red a modo de ejemplo de la figura 8C, un ejemplo en el que el dispositivo A responde con una selección de traspaso de NFC que incluye una información de conexión, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8E ilustra el diagrama de red a modo de ejemplo de la figura 8D, un ejemplo en el que el dispositivo A envía una trama de gestión con un elemento de información (IE) de configuración protegida de Wi-Fi (WSC) al AP/GO de dispositivo central en un procedimiento de configuración protegida de Wi-Fi. El elemento de información (IE) de WSC de incluye la información de autenticación que será reconocible por el AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8F ilustra el diagrama de red a modo de ejemplo de la figura 8E, un ejemplo en el que el dispositivo B emite una trama de solicitud, por ejemplo, una trama de solicitud de sondeo con un elemento de información (IE) de configuración protegida de Wi-Fi (WSC), enviando la misma al AP/GO de dispositivo central en un procedimiento de configuración protegida de Wi-Fi, que incluye la información de autenticación reconocible por el AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8G ilustra el diagrama de red a modo de ejemplo de la figura 8F, en el que el AP/GO de dispositivo central reconoce la información de autenticación que sirve como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. El AP/GO de dispositivo central concede un acceso de red al dispositivo B y envía credenciales al dispositivo B, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8H ilustra el diagrama de red a modo de ejemplo de la figura 8G, en el que el dispositivo B está ahora conectado a la red con su nueva configuración y se puede comunicar con el dispositivo A a través de la red, a través del AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8I ilustra el diagrama de red a modo de ejemplo de la figura 8B, de un ejemplo alternativo en el que el dispositivo A transmite una solicitud de traspaso de NFC que incluye una información de conexión, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8J ilustra el diagrama de red a modo de ejemplo de la figura 8I, de un ejemplo alternativo en el que el dispositivo B está respondiendo con una selección de traspaso de NFC al dispositivo A que incluye una información de autenticación, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 9A es una realización a modo de ejemplo de un mensaje de solicitud de traspaso de NFC desde el dispositivo B al dispositivo A con una solicitud de información y que incluye la información de autenticación, para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 9B es una realización a modo de ejemplo un mensaje de selección de traspaso de NFC enviado desde el dispositivo A al dispositivo B para proporcionar ajustes de conectividad para obtener un acceso de red a través del AP/GO de dispositivo central, de acuerdo con una realización de la presente invención.

La figura 9C es una realización alternativa a modo de ejemplo de un mensaje de solicitud de traspaso de NFC enviado desde el dispositivo A al dispositivo B en la figura 8I, para proporcionar ajustes de conectividad para obtener un acceso de red a través del AP/GO de dispositivo central, de acuerdo con una realización de la presente invención.

La figura 9D es una realización alternativa a modo de ejemplo de un mensaje de selección de traspaso de NFC enviado desde el dispositivo B al dispositivo A en la figura 8J, que incluye la información de autenticación, para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 10 ilustra una trama de gestión de IEEE 802.11 a modo de ejemplo enviada por el dispositivo A al AP/GO de dispositivo central con la información de autenticación en un elemento de información de WSC, de acuerdo con una realización de la presente invención.

La figura 11A es un diagrama de flujo a modo de ejemplo de etapas operativas de una realización a modo de ejemplo del método llevado a cabo por el dispositivo A de la figura 2 y las figuras 8A - 8H, de acuerdo con una realización de la presente invención.

La figura 11B es un diagrama de flujo a modo de ejemplo de etapas operativas de una realización a modo de ejemplo del método llevado a cabo por el dispositivo B de la figura 2 y las figuras 8A - 8H, de acuerdo con una realización de la presente invención.

La figura 11C es un diagrama de flujo a modo de ejemplo de etapas operativas de una realización a modo de ejemplo del método llevado a cabo entre el dispositivo A, el dispositivo B y el AP/GO de dispositivo central de la figura 2, la figura 4 y las figuras 8A - 8H, de acuerdo con una realización de la presente invención.

ANÁLISIS DE REALIZACIONES A MODO DE EJEMPLO DE LA INVENCIÓN:

Esta sección está organizada en los siguientes temas:

A. Tecnología de comunicación de WLAN - P. 11

1. WLAN de IEEE 802.11

2. Configuración protegida de Wi-Fi / configuración simple de Wi-Fi (WSC)

3. Autenticación en configuración protegida de Wi-Fi / configuración simple de Wi-Fi

4. Wi-Fi Direct - puntos de acceso de soporte lógico

B. Tecnología de comunicación de campo cercano (NFC) - P. 23

C. Traspaso de conexión de NFC a WLAN -P. 25

D. Configuración de conexión fuera de banda con dispositivo de punto de acceso o de propietario de grupo - P. 26

A. TECNOLOGÍA DE COMUNICACIÓN DE WLAN

1, WLAN DE IEEE 802.11

La norma IEEE 802.11 especifica métodos y técnicas de una operación de red de área local inalámbrica (WLAN) a modo de ejemplo. Los ejemplos incluyen las especificaciones de red de área local inalámbrica de IEEE 802.11b y 802.11 g, que han sido una tecnología básica para las aplicaciones de WLAN tradicionales en la banda de ISM de 2,4 GHz. Las diversas modificaciones a la norma IEEE 802.11 se consolidaron para los protocolos IEEE 802.11a, b, d, e, g, h, i, j, en la norma base IEEE 802.11-2007, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, junio de 2007. Desde entonces, las emergentes aplicaciones de banda ancha han estimulado el interés en el desarrollo de redes inalámbricas de muy alta velocidad para la comunicación de corto alcance, por ejemplo, las especificaciones de WLAN de IEEE 802.11 n, las especificaciones de WLAN de IEEE 802.11ac planificadas y las especificaciones de WLAN de IEEE 802.11 ad planificadas que han de proporcionar un caudal muy alto en bandas de frecuencia más altas. Las aplicaciones de estas normas IEEE 802.11 incluyen productos tales como electrónica de consumo, teléfonos, ordenadores personales y puntos de acceso tanto para el hogar como para la oficina.

Una WLAN de IEEE 802.11 se puede organizar como un conjunto de servicios básicos independientes (IBSS) o un conjunto de servicios básicos (BSS) de infraestructura. El punto de acceso (AP) en una red WLAN de IEEE 802.11 de conjunto de servicios básicos (BSS) de infraestructura, es un nodo centralizado que ha de retransmitir toda la comunicación entre los dispositivos inalámbricos móviles (STA) en un BSS de infraestructura. Si una STA en un BSS de infraestructura desea comunicar una trama de datos a una segunda STA, la comunicación ha de realizar dos saltos. En primer lugar, la STA de origen transfiere la trama al AP. En segundo lugar, el AP transfiere la trama a la segunda STA. En un BSS de infraestructura, el AP o bien transmite balizas o bien responde a los sondeos recibidos desde las STA. Después de una posible autenticación de una STA que es puesta en práctica por el AP, tiene lugar una asociación entre el AP y una STA que posibilita que se intercambie tráfico de datos con el AP. El punto de acceso (AP) en un BSS de Infraestructura puede conectar el tráfico fuera del BSS sobre una red de distribución. Las STA que son miembros del BSS intercambian paquetes solo con el AP.

La WLAN de IEEE 802.11 usa dos tipos de transmisión: función de coordinación distribuida (DCF) y función de coordinación de punto (PCF). DCF emplea acceso múltiple con detección de portadora con evitación de colisión (CSMA/CA). El receptor da un acuse de recibo positivo de cada paquete enviado. Una transmisión comienza con un solicitar para enviar (RTS) y el receptor responde con un liberar para enviar (CTS). El canal es liberado por estos dos mensajes, debido a que todas las STA que oyen el CTS suprimirán su propio inicio de una transmisión. Entonces, cuando se transmiten paquetes de datos, cada uno tiene un vector de atribución de red (NAV) que contiene un valor de duración para reservar el canal para el emisor y el receptor durante un intervalo después del paquete actual, igual a la duración del NAV. El valor del NAV decrece con el paso del tiempo. Una vez que el emisor y el receptor han reservado el canal, lo pueden conservar la duración restante del valor de NAV. El último paquete de acuse de recibo (ACK) contiene un valor de NAV de cero, para liberar inmediatamente el canal. La función de coordinación de punto (PCF) es un método de interrogación entre las STA del BSS, que es coordinado por el punto de acceso.

La autenticación de IEEE 802.11 opera al nivel de enlace entre las STA de IEEE 802.11. La norma 802.11 de IEEE intenta controlar el acceso de LAN por medio del servicio de autenticación. La autenticación de IEEE 802.11 es un servicio de estación que puede ser usado por todas las STA para establecer su identidad para las STA con las que se comunican las mismas en las redes tanto de infraestructura como de IBSS. Si no se ha establecido un nivel mutuamente aceptable de autenticación entre dos STA, entonces no se establece una asociación. IEEE 802.11 define dos métodos de autenticación: autenticación de sistema abierta y autenticación de clave compartida. la autenticación de sistema abierta admite cualquier STA en el sistema de distribución. La autenticación de clave compartida depende de una privacidad equivalente a la cableada para mostrar conocimiento de una clave de cifrado. El mecanismo de autenticación de IEEE 802.11 también permite la definición de nuevos métodos de autenticación. Una asociación de red de seguridad robusta (RSNA) soporta autenticación basándose en IEEE 802.1X-2004, o claves precompartidas (PSK). La autenticación de IEEE 802.1X utiliza el protocolo de autenticación extensible (EAP) (IETF RFC 3748-2004) para autenticar las STA y un servidor de autenticación (AS) entre sí. En IEEE 802.1X, una STA que se está autenticando y el dispositivo autenticador intercambian información de protocolo por medio del puerto no controlado de IEEE 802.1X. Se bloquea el paso por parte del puerto controlado de IEEE 802.1X de tráfico de datos generales entre dos STA hasta que un procedimiento de autenticación de IEEE 802.1X se completa con éxito a través del puerto no controlado de IEEE 802.1X.

2. Configuración protegida de Wi-Fi / configuración simple de Wi-Fi (WSC)

La configuración de red para las WLAN de IEEE 801.11 ha sido simplificada por el sistema de configuración protegida de Wi-Fi™ que se incluye en la mayor parte de los puntos de acceso. La Alianza Wi-Fi publicó la especificación de configuración protegida de Wi-Fi (WPS) 1.0, *Wi-Fi Protected Setup Specification* versión 1.0h, diciembre de 2006. El documento *Wi-Fi Simple Configuration (WSC) Specification*, versión 2.0, 20 de diciembre de 2010, (incorporada en el presente documento por referencia), actualiza el documento *Wi-Fi Protected Setup Specification*, versión 1.0h. El acrónimo WSC, para el documento *Wi-Fi Simple Configuration Specification*, se puede usar de forma intercambiable con el acrónimo WPS, para la configuración protegida de Wi-Fi. La configuración protegida de Wi-Fi facilita la configuración inicial de los dispositivos de IEEE 802.11 en una red de infraestructura de Wi-Fi de tal modo que los mismos se pueden configurar más fácilmente con características de seguridad y de tal modo que esos nuevos dispositivos de Wi-Fi se pueden añadir a la red. La configuración protegida de Wi-Fi permite que se configuren puntos de acceso mediante la introducción de un PIN. El sistema de configuración protegida usa esta información para enviar datos a un ordenador conectado al punto de acceso, para completar la configuración de red. La configuración protegida de Wi-Fi define nuevos elementos de información de IEEE 802.11 (IE) que se incluyen en balizas, solicitudes de sondeo y respuestas de sondeo. El fin de estos IE es anunciar la presencia de dispositivos que son capaces de realizar operaciones de configuración protegida de Wi-Fi.

El descubrimiento inicial de los dispositivos de configuración simple de Wi-Fi se logra usando elementos de información de IEEE 802.11 en tramas de gestión (baliza, solicitud de sondeo y respuesta de sondeo). Si el inscrito decide perseguir una conexión a la red, inicia una conexión de IEEE 802.1X/EAP para el protocolo de registro basado en el protocolo de autenticación extensible (EAP). El elemento de información de configuración de Wi-Fi Simple es conforme con el formato de elemento de información de IEEE 802.11 e indica datos específicos necesarios para la información, capacidades y modos de red, para configurar un inscrito para la red inalámbrica y para notificar problemas con el inscrito asociándose con una red inalámbrica especificada con los ajustes suministrados.

La norma de configuración protegida de Wi-Fi 1.0 define tres tipos de componentes en una red: un registrador, un inscrito y un punto de acceso (AP). Un registrador es un componente con la autoridad para emitir y revocar credenciales para una red. Un registrador se puede integrar en un AP o el mismo se puede encontrar separado del AP. Un inscrito es un componente que está tratando de unirse a una red LAN inalámbrica. Un autenticador es un AP que funciona como un representante entre un registrador y un inscrito. Un dispositivo inalámbrico del registrador configura el dispositivo inalámbrico del inscrito, y el AP actúa como un autenticador para redirigir mediante representante los mensajes relevantes entre el registrador y el inscrito. Los mensajes intercambiados en la sesión son una serie de mensajes de solicitud/respuesta del protocolo de autenticación extensible (EAP), terminando con el inscrito reconectándose con la red con su nueva configuración. EAP es un marco de autenticación definido en RFC 5247, para proporcionar el transporte y el uso de material de modulación y parámetros necesarios para establecer una red de Wi-Fi segura. El documento *Wi-Fi Simple Configuration Specification*, versión 2.0, 20 de diciembre de 2010, actualiza el documento *Wi-Fi Protected Setup Specification*, versión 1.0h.

Un AP autónomo que soporta configuración protegida de Wi-Fi, incluye un registrador integrado y no usa un registrador externo. En la configuración de WLAN inicial con configuración protegida de Wi-Fi, cuando se inicializa en un modo autónomo, un AP de configuración protegida de Wi-Fi elige automáticamente un canal y SSID aleatorio. Un AP autónomo que incluye un registrador de configuración protegida de Wi-Fi, emite claves a los inscritos por medio del protocolo de registro.

Cuando se inicializa un inscrito, Busca balizas desde los AP y envía solicitudes de sondeo con el elemento de información (IE) de WSC, o bien a redes seleccionadas o bien a cada red de forma secuencial. Este también puede enviar solicitudes de sondeo a cada canal de IEEE 802.11 con el IE de WSC incluido. Busca el IE de WSC en las respuestas de sondeo que recibe y puede entrar en contacto con uno o más registradores para descubrir adicionalmente capacidades de registrador y para ver si el usuario ha seleccionado un registrador. El inscrito puede continuar buscando indicadores de registrador seleccionados en balizas, respuestas de sondeo y cualquier mensaje M2 y puede dejar de explorar cuando halla un registrador que indica que está preparado para configurar el inscrito.

El siguiente ejemplo describe un procedimiento de configuración dentro de banda a modo de ejemplo usando la configuración protegida de Wi-Fi para añadir dispositivos miembros usando un AP/registrador autónomo. el usuario puede llevar la contraseña de dispositivo del inscrito al AP/registrador usando una entrada de teclado o un canal fuera de banda con traspaso de conexión de comunicación de campo cercano (NFC). Este ejemplo no muestra el intercambio de mensajes M1 y M2D preliminares que puede tener lugar después del intercambio de mensaje de sondeo, debido a que el inscrito puede estar esperando a que el usuario configure el AP/registrador con la contraseña de dispositivo del inscrito.

1. El inscrito envía sus datos de descubrimiento en una solicitud de sondeo a un AP de configuración protegida de Wi-Fi o un registrador inalámbrico *ad hoc*. El AP o el registrador inalámbrico responde con sus propios datos de descubrimiento en la respuesta de sondeo.

2. se puede inducir al usuario a introducir la contraseña de dispositivo del inscrito en el AP/registrador usando una interfaz de teclado numérico o un canal fuera de banda.

3. El inscrito se conecta e inicia el procedimiento de control de acceso de red basado en puerto de IEEE 802.1X para una autenticación basada en puerto.

4. El inscrito y el registrador intercambian mensajes M1-M8 para aprovisionar al inscrito.

5. El inscrito se desasocia y se reconecta, usando su nueva credencial de autenticación de WLAN. El inscrito está conectado ahora a la red con su nueva configuración.

3. Autenticación en configuración protegida de Wi-Fi/configuración simple de Wi-Fi

El documento *Wi-Fi Simple Configuration Specification*, versión 2.0 (renombrado a partir del nombre original "*Wi-Fi Protected Setup*"), usa la autenticación basada en puerto de IEEE 802.1X y el protocolo de autenticación extensible (EAP) para transportar mensajes de protocolo de registro en banda. Este protocolo se asigna en un método de EAP personalizado que se describe en lo sucesivo. La configuración simple de Wi-Fi no requiere que el AP soporte el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) (IETF RFC 2865-2000), y no es necesario que la red incluya un servidor de autenticación. De hecho, muchos AP de configuración simple de Wi-Fi pueden soportar IEEE 802.1X solo para configurar las credenciales personales de acceso protegido de Wi-Fi 2 (WPA2) usando la configuración simple de Wi-Fi. A los inscritos que hacen uso de la configuración simple de Wi-Fi no se les concede un acceso directo a la WLAN a través del método de EAP personalizado de la configuración simple de Wi-Fi. El método de EAP se usa para configurar el inscrito con una credencial que se puede usar posteriormente con cualquier método de acceso que sea soportado por esa WLAN. Por ejemplo, si el AP solo soporta WPA2-Personal con una clave precompartida (PSK) compartida en toda la red, entonces el inscrito ejecutaría el intercambio de 802.1X para obtener la PSK, se desasociaría y, entonces, se reconectaría y usaría WPA2-Personal para acceder a la WLAN. Como alternativa, si el AP soporta la autenticación de 802.1X, el inscrito puede en primer lugar ejecutar el método de EAP de la configuración de Wi-Fi Simple para obtener una credencial de secreto compartido y, entonces, reconectarse usando ese secreto junto con otro método de EAP para acceder a la WLAN.

El método de EAP de la configuración de Wi-Fi Simple (EAP-WSC) se puede usar para el descubrimiento de registradores y de inscritos y para el establecimiento de credenciales. La primera vez que el inscrito encuentra una nueva WLAN, este envía al exterior su información de descubrimiento y ejecuta el método de EAP-WSC. Tanto en el mensaje de descubrimiento como en el mensaje de protocolo de registro M1, el inscrito proporciona información acerca de sí mismo a la WLAN. De forma similar, los mensajes M2 y M2D enviados al inscrito proporcionan información acerca de los registradores disponibles. Cuando por primera vez el inscrito descubre e intenta conectar con la WLAN, puede que el registrador o registradores de la WLAN no conozcan aún la contraseña de dispositivo del inscrito. Por lo tanto, los registradores sin la contraseña de dispositivo responden con mensajes M2D. Aunque estos mensajes M2D no están autenticados, estos pueden ayudar a los inscritos con interfaces de usuario sofisticadas, para guiar al usuario a través del proceso de inscripción.

Cuando el inscrito realiza una exploración sobre los mensajes M2D enviados por la red, este puede descubrir que ninguno de los mismos posee su contraseña de dispositivo. En este punto, el inscrito tiene una oportunidad de inducir al usuario a realizar una operación de arranque de confianza tal como conectar un canal fuera de banda disponible o introducir una contraseña de dispositivo en uno de los registradores disponibles. Si el usuario decide introducir la contraseña de dispositivo del inscrito en el registrador, el inscrito se puede reconectar y ejecutar el método de EAP una vez más para realizar el protocolo de registro completo. Si el inscrito no tiene interfaz de usuario alguna para guiar al usuario a través de la inscripción, es probable que uno o más de los registradores de las WLAN pueda hacer esto. Tanto al registrador como al inscrito se les da suficiente información acerca de las capacidades del otro a través del método de EAP para guiar con éxito al usuario a través de la inscripción. Si el usuario decide usar un canal fuera de banda para el registro, entonces el mensaje M2 es autenticado implícitamente por el canal y puede portar los datos de configuración de red.

El AP funciona como el autenticador de EAP en la WLAN. De esta manera, el AP genera mensajes de solicitud de EAP y los inscritos y registradores generan respuestas de EAP. Si el registrador es externo al AP, entonces este usa conexión de tipo enchufar y usar universal (UPnP, *plug and play universal*) para intercambiar mensajes de protocolo de registro con el AP. Un registrador también puede funcionar en el papel de un autenticador de 802.1X, que es útil para redes con AP heredados.

El método de EAP de la configuración de Wi-Fi Simple usa EAP, tal como se especifica en RFC 3748, y el protocolo de autenticación extensible (EAP) a través de LAN (EAPoL), tal como se especifica en IEEE 802.1X-2001, pero no representa un protocolo de autenticación de red. En lugar de la configuración de Wi-Fi Simple, utiliza la conexión de datos de 802.1X para adquirir ajustes necesarios para conectar con la red y el intercambio de EAP resultante siempre ha de terminar con un fallo de EAP.

Cuando el inscrito decide conectar con la red y ejecutar el método de EAP de la configuración simple de Wi-Fi, este se asocia con el AP y envía un mensaje de inicio de EAPoL. El AP responde con una solicitud/identidad de EAP. El inscrito envía una respuesta/identidad de EAP que contiene el nombre definido de la Alianza Wi-Fi para un inscrito de configuración simple ("WFA-SimpleConfig-Enrollee-1-0"). Esto da lugar a que el AP comience a ejecutar el método de EAP de configuración simple. Los mensajes de protocolo de registro se intercambian hasta que M8 ha sido recibido y validado por el inscrito. Si procesa con éxito M8, el inscrito envía un mensaje de respuesta/realizado de EAP al autenticador, que envía el mensaje de WSC_realizado a cualquier registrador externo y el autenticador devuelve un mensaje de fallo de EAP al inscrito. Un inscrito debería suponer que las credenciales recibidas son válidas después de procesar con éxito el mensaje M8 y de enviar el mensaje de WSC_realizado. El inscrito se desasocia entonces y se reconecta con la credencial obtenida de los datos de config. del M8. Si M2D es recibido por el inscrito, este debería responder con un mensaje de ACK de tal modo que el AP puede continuar enviándole mensajes de descubrimiento procedentes de otros registradores. Después de que el AP haya enviado un fallo de EAP al inscrito, el inscrito puede hacer una de dos cosas (dado que el AP no desautenticó el inscrito después de enviar el fallo de EAP): este se puede desconectar del AP y reconectarse un cierto tiempo más tarde para volver a ejecutar el método de EAP de la configuración simple de Wi-Fi mediante el envío de un mensaje de inicio de EAPoL o puede permanecer conectado al AP y volver a ejecutar el método de EAP de la configuración simple de Wi-Fi mediante el envío de otro mensaje de inicio de EAPoL.

Una vez que el inscrito ha enviado un mensaje M3, tanto el registrador como el inscrito han de proceder de una forma al compás o bien hasta que tiene lugar un fallo o bien hasta que tiene lugar un éxito (indicado por el mensaje de respuesta de Realizado). Si el inscrito (el suplicante de IEEE 802.1X) detecta cualquier error en estas últimas fases, responde mediante el envío de un mensaje de NACK y la realización de una transición al estado de terminación para terminar la conexión. En este punto, el inscrito computa una contraseña de dispositivo nueva para su uso en la siguiente instancia del protocolo de registro. Si se reutiliza la misma contraseña con múltiples instancias del protocolo, esta será susceptible a un ataque activo.

Los mensajes de protocolo de registro M1 a M8 se describen en el documento *Wi-Fi Simple Configuration Specification*, versión 2.0. Incluyen un intercambio de claves públicas, descripción del dispositivo emisor, incluyendo su dirección de MAC y capacidades de dispositivo, y diversos valores de autenticación de mensaje, culminando con el envío por parte del registrador al inscrito de credenciales para acceder a la red.

Una credencial es una estructura de datos emitida por un registrador a un inscrito, que permite que este último obtenga acceso a la red. Con una configuración fuera de banda, se envían credenciales de WLAN a través del canal fuera de banda al inscrito. Las interfaces de NFC que operan en un modo punto a punto entre un AP o propietario de grupo (GO) que tiene un registrador integrado y un dispositivo inscrito, tienen las propiedades de seguridad más robustas soportadas por el documento *Wi-Fi Simple Configuration Specification*, debido a que los ataques prácticos de tipo intermediario contra la NFC no resultan factibles. En este modo, se realiza un intercambio de Diffie-Hellman de 1536 bits a través de la interfaz de NFC, y los ajustes de WLAN se cifran usando la norma de cifrado avanzada (AES) de 128 bits y se entregan a través de la misma interfaz entre un AP o propietario de grupo (GO) y un dispositivo inscrito. Las claves públicas de Diffie-Hellman y los ajustes de WLAN son autenticados implícitamente tanto por el registrador como por el inscrito, debido a que estos se reciben a través del canal de NFC.

La credencial que se muestra en la siguiente tabla 1, es un atributo compuesto emitido por un AP o propietario de grupo (GO) que tiene un registrador integrado, que representa una única credencial de WLAN. Puede haber múltiples instancias del atributo de credencial. El documento *Wi-Fi Simple Configuration Specification* proporciona la siguiente tabla que enumera los atributos en credenciales ("R" quiere decir requerido y "0" quiere decir opcional):

Tabla 1 - Credencial

Atributo		**R/O**		**Notas, Valores permitidos**	
1.	Índice de red	2.	R	3.	Desaconsejado - usar el valor fijo 1 para la compatibilidad con versiones anteriores.
4.	SSID	5.	R	6.	SSID de red.
7.	Tipo de autenticación	8.	R	9.	El tipo de autenticación usado en esta red.
10.	Tipo de cifrado	11.	R		12. El tipo de cifrado usado en esta red.
13.	Índice de clave de red	14.	O	15.	Desaconsejado. Solo incluido por los dispositivos de WSC 1.0. Ignorado por los dispositivos de WSC 2.0 o más nuevos.
16.	Clave de red	17	R	18.	
19.	Dirección de MAC	20	R	21.	Dirección de MAC de un dispositivo miembro.
22.	Tipo de EAP	23.	O	24.	

Atributo		R/O		Notas, Valores permitidos	
25.	Identidad de EAP	26.	O	27.	
28.	Clave proporcionada automáticamente	29.	O	30.	
31.	802.1X habilitado	32	O	33.	
34.	clave de red compartible (en el interior de la extensión de fabricante de WFA)	35.	O	36.	Si se encuentra presente, este atributo indica si la clave de red se puede compartir, o no, con otros dispositivos.
37.	<otros...>	38.	O	39.	Se permiten múltiples atributos.

4. Wi-Fi Direct - puntos de acceso de soporte lógico

La Alianza Wi-Fi ha desarrollado una tecnología punto a punto de Wi-Fi denominada Wi-Fi Direct™ que se especifica en el documento *Wi-Fi Alliance Peer-to-Peer Specification*, octubre de 2010. Wi-Fi Direct, a la que también se hace referencia en el presente documento como punto a punto o P2P. Wi-Fi Direct posibilita que los dispositivos de IEEE 802.11a, g o n se conecten entre sí, punto a punto, sin configuración anterior o la necesidad de puntos de acceso inalámbricos. Wi-Fi Direct incrusta un punto de acceso de soporte lógico en cualquier dispositivo, que proporciona una versión de la configuración protegida de Wi-Fi. Cuando un dispositivo entra dentro del alcance de una STA que soporta Wi-Fi Direct (un dispositivo de Wi-Fi Direct), se puede conectar a la misma y, entonces, recopilar información de configuración usando una transferencia de configuración protegida de Wi-Fi. Los dispositivos que soportan Wi-Fi Direct se pueden descubrir unos a otros y anunciar los servicios disponibles. Los dispositivos de Wi-Fi Direct soportan los intervalos de Wi-Fi típicos y las mismas tasas de datos que se pueden lograr con una conexión de infraestructura de 802.11a, g o n. Cuando un dispositivo entra dentro del alcance del dispositivo de Wi-Fi Direct, se puede conectar al mismo usando el protocolo existente y, entonces, recopilar información de configuración usando una transferencia de configuración protegida de Wi-Fi 2.0.

Wi-Fi Direct posibilita que los dispositivos de IEEE 802.11 que soportan Wi-Fi Direct, se conecten entre sí, punto a punto, sin unirse a una red. La especificación se puede poner en práctica en cualquier dispositivo de Wi-Fi. Los dispositivos que soportan la especificación serán capaces de descubrirse unos a otros y de anunciar los servicios disponibles. Los dispositivos de Wi-Fi Direct soportarán los intervalos de Wi-Fi típicos y las mismas tasas de datos que se pueden lograr con una conexión de infraestructura. Wi-Fi Direct proporciona conexiones punto a punto para redes mediante la incrustación de un punto de acceso de soporte lógico en cualquier dispositivo que desee soportar Wi-Fi Direct. El AP de soporte lógico proporciona una versión de la configuración protegida de Wi-Fi 1.0 mediante la introducción de un PIN o al pulsar un botón. Cuando un dispositivo entra dentro del alcance del dispositivo de Wi-Fi Direct, se puede conectar al mismo usando el protocolo existente y, entonces, recopilar información de configuración usando una transferencia de configuración protegida de Wi-Fi 1.0.

Los dispositivos certificados para Wi-Fi Direct pueden crear conexiones directas entre dispositivos de cliente de Wi-Fi sin requerir la presencia de una red de infraestructura de Wi-Fi tradicional de un punto de acceso o encaminador. Los dispositivos certificados para Wi-Fi Direct soportan la conexión a dispositivos de Wi-Fi heredados existentes usando los protocolos de IEEE 802.11 a/g/n. Las características de descubrimiento de servicios y de descubrimiento de dispositivos de Wi-Fi Direct permiten que los usuarios identifiquen los dispositivos y servicios disponibles antes de establecer una conexión, por ejemplo, descubrir qué redes de Wi-Fi tienen una impresora. Los dispositivos de Wi-Fi Direct pueden usar la configuración protegida de Wi-Fi para crear conexiones entre dispositivos.

Un dispositivo de Wi-Fi Direct es capaz de una conexión punto a punto y puede soportar o bien una red de infraestructura de un punto de acceso o encaminador o bien una conexión punto a punto (P2P). Los dispositivos de Wi-Fi Direct se pueden unir a las redes de infraestructura como estaciones (STA) y pueden soportar una funcionalidad de inscrito de configuración protegida de Wi-Fi. Los dispositivos de Wi-Fi Direct se pueden conectar mediante la formación de grupos en una topología de uno a uno o de uno a muchos. Los grupos funcionan de una forma similar a la de un conjunto de servicios básicos (BSS) de infraestructura. Un único dispositivo de Wi-Fi Direct será el propietario de grupo (GO) que gestiona el grupo, incluyendo controlar a qué dispositivos se les permite unirse y cuándo se inicia o se termina el grupo. El propietario de grupo (GO) aparecerá como un punto de acceso a dispositivos de cliente heredados.

Los dispositivos de Wi-Fi Direct incluyen una funcionalidad de registrador interno de configuración protegida de Wi-Fi y una comunicación entre clientes en el grupo. Los dispositivos de Wi-Fi Direct pueden ser un propietario de grupo (GO) de un grupo y pueden ser capaces de negociar qué dispositivo adopta este papel cuando se forma un grupo con otro dispositivo de Wi-Fi Direct. Un grupo puede incluir tanto dispositivos de Wi-Fi Direct como dispositivos heredados (es decir, que no son conformes con el documento *Wi-Fi Alliance Peer-to-Peer Specification*). Los dispositivos heredados solo pueden funcionar como clientes dentro de un grupo.

Los dispositivos de Wi-Fi Direct pueden soportar mecanismos de descubrimiento. El descubrimiento de dispositivos se usa para identificar otros dispositivos de Wi-Fi Direct y establecer una conexión mediante el uso de una exploración similar a la usada para descubrir puntos de acceso de infraestructura. Si el objetivo no es parte ya de un grupo, se puede formar un nuevo grupo. Si el objetivo es parte ya de un grupo, el dispositivo de Wi-Fi Direct que está buscando puede intentar unirse al grupo existente. La configuración protegida de Wi-Fi se puede usar para obtener credenciales desde el propietario de grupo (GO) y autenticar el dispositivo de Wi-Fi Direct que está buscando. Los dispositivos de Wi-Fi Direct puede incluir el descubrimiento de servicios que posibilita el anuncio de servicios soportados por aplicaciones de capas superiores a otros dispositivos de Wi-Fi Direct. El descubrimiento de servicios se puede realizar en cualquier momento (por ejemplo, incluso antes de que se haya formado una conexión) con cualquier otro dispositivo de Wi-Fi Direct descubierto.

Un grupo puede ser creado por un único dispositivo de Wi-Fi Direct, tal como cuando se conecta un dispositivo heredado. Cuando se forma una conexión entre dos dispositivos de Wi-Fi Direct, un grupo se puede formar automáticamente y los dispositivos pueden negociar para determinar qué dispositivo es el propietario de grupo. El propietario de grupo puede decidir si este es un grupo temporal (de única instancia) o persistente (de uso múltiple y recurrente). Después de que se haya formado un grupo, un dispositivo de Wi-Fi Direct puede invitar a otro dispositivo de Wi-Fi Direct a unirse al grupo. La decisión de si aceptar, o no, una invitación, se puede dejar en manos del dispositivo de Wi-Fi Direct invitado.

Los dispositivos de Wi-Fi Direct concurrente pueden participar en múltiples grupos, de forma simultánea, cada grupo requiere una pila de Wi-Fi propia. Un dispositivo de Wi-Fi Direct que se puede encontrar en un grupo mientras se mantiene una conexión de infraestructura de WLAN al mismo tiempo se considera un dispositivo concurrente o un dispositivo de pila doble. Por ejemplo, un ordenador portátil conectado directamente a una impresora al tiempo que, de forma simultánea, se usa una conexión de WLAN, está operando como un dispositivo concurrente. Las conexiones concurrentes pueden ser soportadas por una única radio y pueden soportar conexiones en diferentes canales. La operación concurrente puede ser soportada por múltiples pilas de protocolos, por ejemplo, una para operación como una STA de WLAN y una para operar como un dispositivo de Wi-Fi Direct. Por ejemplo, se pueden mantener dos entidades de MAC físicas separadas, cada una asociada con su propia entidad de PHY, o pueden usar una única entidad de PHY que soporta dos entidades de MAC virtuales.

El documento *Wi-Fi Peer-to-Peer Technical Specification* v1.1, 2010 publicado por la Alianza Wi-Fi, prevé el aprovisionamiento en las redes de Wi-Fi Direct. El aprovisionamiento es una fase de formación de grupo punto a punto en la que las credenciales para el grupo punto a punto se intercambian basándose en el uso de la configuración simple de Wi-Fi. Las credenciales son información que se requiere para unirse a un grupo punto a punto tal como se define en el documento *Wi-Fi Simple Configuration Specification*.

Para prever la configuración de dispositivos punto a punto, los dispositivos punto a punto pueden retardar el comienzo de la fase de aprovisionamiento hasta la expiración del mayor del tiempo de configuración del propietario de grupo (GO) punto a punto y el tiempo de configuración de cliente del cliente punto a punto, basándose en unos atributos respectivos de temporización de configuración intercambiados durante una negociación de propietario de grupo precedente.

El dispositivo punto a punto seleccionado como un propietario de grupo (GO) punto a punto durante la negociación de propietario de grupo puede empezar una sesión de grupo punto a punto usando las credenciales que este pretende usar para ese grupo. El propietario de grupo (GO) punto a punto puede usar el canal operativo que se indica durante la negociación de propietario de grupo, si se encuentra disponible. El cliente punto a punto se puede conectar al propietario de grupo punto a punto para obtener credenciales. Si el canal operativo no se encuentra disponible, el propietario de grupo punto a punto puede usar otro canal a partir de un atributo de lista de canales enviado en la trama de confirmación de negociación de propietario de grupo. El cliente punto a punto puede tener que explorar para hallar al propietario de grupo punto a punto si el canal operativo previsto no se encuentra disponible. Un bit de formación de grupo en un mapa de bits de capacidad de grupo punto a punto del atributo de capacidad punto a punto se puede ajustar a uno hasta que tiene éxito el aprovisionamiento.

El aprovisionamiento se puede ejecutar en las redes de Wi-Fi Direct, tal como se describe, por ejemplo, en el documento *Wi-Fi Simple Configuration (WSC) Specification*, versión 2.0, 20 de diciembre de 2010. El propietario de grupo (GO) punto a punto puede desempeñar el papel del punto de acceso con un registrador interno. Este solo permitirá la asociación por el dispositivo punto a punto con el que este se encuentra en la actualidad en una formación de grupo. Ya que el usuario ha introducido el PIN de WSC o desencadenado la funcionalidad de botón pulsador de WSC en ambos dispositivos, el registrador puede enviar un mensaje M2 en respuesta a un mensaje M1. El cliente punto a punto puede desempeñar el papel del inscrito de STA. Este se puede asociar con el dispositivo punto a punto con el que este se encuentra en la actualidad en la formación de grupo.

Si falla el aprovisionamiento, entonces la formación de grupo termina y el propietario de grupo (GO) punto a punto puede terminar la sesión de grupo punto a punto. Si falla el aprovisionamiento, el dispositivo punto a punto puede volver a intentar la formación de grupo o volver al descubrimiento de dispositivos. Cuando se completa con éxito el aprovisionamiento en las redes de Wi-Fi Direct, el propietario de grupo (GO) punto a punto puede ajustar el bit de

formación de grupo en el mapa de bits de capacidad de grupo punto a punto del atributo de capacidad punto a punto a cero. En este punto, el cliente punto a punto se puede unir al grupo punto a punto en la red de Wi-Fi Direct, usando las credenciales suministradas durante el aprovisionamiento.

B. Tecnología de comunicación de campo cercano (NFC)

Uno de los métodos proporcionados por el documento *Wi-Fi Simple Configuration Specification*, versión 2.0, es el método de comunicación de campo cercano (NFC), en el que el usuario pone un nuevo dispositivo de cliente inalámbrico (STA) cerca de un punto de acceso (AP) o registrador de la red para permitir una comunicación de campo cercano entre los dispositivos.

Las tecnologías de comunicación de campo cercano, tales como las tecnologías de identificación por radiofrecuencia (RFID), comprenden una gama de sistemas de transmisión por RF, por ejemplo, sistemas normalizados y patentados para un gran número de fines diferentes, tales como el etiquetado de productos para gestión de inventario y logística, fines de evitación de robos en el punto de venta y reciclaje de productos al final del ciclo de vida del producto etiquetado. Además de las tecnologías de RFID, la tecnología de comunicación de campo cercano (NFC) ha evolucionado recientemente a partir de una combinación de las tecnologías de identificación y de interconexión sin contacto existentes. NFC es una tecnología tanto de "lectura" como de "escritura". la comunicación entre dos dispositivos compatibles con NFC tiene lugar cuando estos se ponen muy próximos uno de otro: Una simple onda o toque puede establecer una conexión de NFC, que es entonces compatible con otras tecnologías inalámbricas conocidas, tal como Bluetooth™ o red de área local inalámbrica (WLAN).

La tecnología de comunicación de campo cercano (NFC) usada en la norma de configuración protegida de Wi-Fi (WPS), se comunica entre dos dispositivos de NFC o entre un dispositivo de NFC y una etiqueta de NFC por medio de una inducción de campo magnético, en donde dos antenas de cuadro se encuentran cada una dentro del campo cercano de la otra, activando de forma eficaz un contacto inalámbrico mediante la formación de un transformador de núcleo de aire. Una radio de NFC a modo de ejemplo opera dentro de la banda de ISM de radiofrecuencia sin licencia de 13,56 MHz, con un ancho de banda de aproximadamente 2 MHz a lo largo de una distancia típica de unos pocos centímetros. La radio de NFC se puede fijar a un nuevo dispositivo de cliente inalámbrico (STA) y el usuario pone la radio de NFC en el dispositivo cerca de un punto de acceso (AP) o registrador de la red para permitir una comunicación de campo cercano entre los dispositivos.

La tecnología de NFC es una ampliación de la norma de tarjetas de proximidad de la norma ISO/IEC 14443 para tarjetas inteligentes sin contacto y dispositivos de ID de radiofrecuencia (RFID), que combina la interfaz de una tarjeta inteligente sin contacto y un lector en un único dispositivo, y usa la norma de comunicación de NFC ISO/IEC 18092 para posibilitar una comunicación bidireccional. Una radio de NFC se puede comunicar tanto con los lectores como con las tarjetas inteligentes sin contacto de la norma ISO/IEC 14443 existentes, así como con otros dispositivos de NFC mediante el uso de la norma ISO/IEC 18092. El Foro NFC™, una asociación industrial sin ánimo de lucro, ha publicado especificaciones que posibilitan diferentes modos de operación denominados: emulación de etiquetas, modo de lectura/escritura y comunicación punto a punto. Adicionalmente, el Foro NFC ha definido especificaciones para el formato de intercambio de datos de NFC (NDEF), tipos de etiqueta de NFC, definición de tipos de registro de NFC y especificación de traspaso de conexión. Véase, por ejemplo, el documento *Connection Handover Technical Specification*, Foro NFC™, *Connection Handover* 1.2, NFCForum-TS-ConnectionHandover_1.2, 2010-07-07. La norma ISO/IEC 18092 define modos de comunicación para la interfaz y el protocolo de comunicación de campo cercano (NFCIP-1) usando dispositivos inductivamente acoplados que operan a la frecuencia central de 13,56 MHz para la interconexión de periféricos informáticos. La norma ISO/IEC 18092 especifica esquemas de modulación, codificaciones, velocidades de transferencia y formato de trama de la interfaz de RF, esquemas de inicialización, condiciones requeridas para el control de colisión de datos durante la inicialización, y un protocolo de transporte que incluye métodos de activación de protocolo y de intercambio de datos.

C. Traspaso de conexión de NFC a WLAN

El traspaso básico a una portadora de WLAN almacena parámetros de WLAN y credenciales en etiquetas del Foro NFC como parte de la configuración protegida de Wi-Fi (WPS). La información se almacena en la cabida útil de un registro de formato de intercambio de datos de NFC (NDEF) identificado por el tipo de mime "application/vnd.wfa.wsc", que se conoce como el "registro de WPS". La información de parámetros de LAN inalámbrica y de credenciales proporcionados en el interior de un registro de WPS incluye el identificador de conjunto de servicios de IEEE 802.11 (SSID), autenticación y tipo de cifrado desplegados por la red inalámbrica, la clave de red secreta que una estación inalámbrica necesita para autenticarse con la red, y la dirección de MAC del dispositivo que recibe la configuración (si se desconoce, esta dirección se ajusta a todo ceros). La especificación de configuración protegida de Wi-Fi 1.0 usa el término "registrador" para un dispositivo que es capaz de proporcionar credenciales de WLAN e "inscrito" para un dispositivo que desea unirse a una red inalámbrica.

En el documento *Wi-Fi Simple Configuration Specification*, versión 2.0, 20 de diciembre de 2010, un solicitante de traspaso con capacidad de Wi-Fi puede dar formato a un mensaje de solicitud de traspaso de NFC en el formato de intercambio de datos de NFC (NDEF), que indica que el solicitante es un dispositivo de IEEE 802.11, pero que no

incluye información de configuración alguna. Una solicitud de traspaso se puede enviar por medio del enlace de NFC en al menos dos escenarios: [1] el solicitante puede no haberse unido aún a un dominio inalámbrico o [2] incluso si el solicitante ya es miembro de una red WLAN, un dispositivo del mismo nivel se puede encontrar en una red diferente y, por lo tanto, se requiere un traspaso de conexión para obtener las credenciales del dispositivo del mismo nivel. En la especificación de configuración protegida de Wi-Fi 2.0, el selector de traspaso deduciría a partir de este mensaje que el solicitante de traspaso soporta una radio de IEEE 802.11 certificada de Wi-Fi. En la especificación de configuración protegida de Wi-Fi 2.0, si el selector de traspaso es un dispositivo de Wi-Fi con conectividad inalámbrica, este debería responder con un mensaje de selección de traspaso de NFC en el formato de intercambio de datos de NFC (NDEF), con un registro de configuración que incluye credenciales, tal como índice de red, SSID, tipo de autenticación, tipo de cifrado, clave de red y dirección de MAC.

La especificación de formato de intercambio de datos de NFC (NDEF), *NFC Forum Data Exchange Format (NDEF) Specification*, Foro NFC™, 2006, define un formado de datos común para que los dispositivos de NFC intercambien datos específicos de aplicaciones o de servicios. Un mensaje de NDEF se construye de un número de registros de NDEF, con el primer y el último registro proporcionando marcadores de inicio y de fin de mensaje. Entre dos dispositivos de NFC, los mensajes de NDEF se pueden intercambiar a través del protocolo Protocolo de control de enlace lógico de NFC (LLCP), especificado en el documento *NFC Forum Logical Link Control Protocol Specification*, Foro NFC™, 2009 (incorporado en el presente documento por referencia). La especificación de traspaso de conexión de NFC, *NFC Forum Connection Handover Specification*, Foro NFC™, 07/07/2010, define el intercambio de mensajes de NDEF entre dos dispositivos de NFC en un traspaso negociado para descubrir y negociar tecnologías de comunicación inalámbrica alternativas.

El solicitante de traspaso en la especificación de configuración protegida de Wi-Fi 2.0, usaría entonces, por lo general, el SSID y la clave de red para inscribirse en la misma red de Wi-Fi a la que está conectado el selector de traspaso. Las acciones adicionales dependen de la provisión de una dirección de IP que identifica el selector de traspaso, los servicios disponibles, y la actividad prevista del solicitante de traspaso.

D. Configuración de conexión fuera de banda con dispositivo de punto de acceso o de propietario de grupo

Algunas realizaciones a modo de ejemplo de la invención posibilitan una conmutación de transporte de portadora de comunicación de corto alcance fuera de banda para la configuración de conexión en una comunicación de dispositivo a dispositivo o bien con un dispositivo de punto de acceso (AP) en una red de infraestructura o bien con un dispositivo de propietario de grupo (GO) en una red P2P. La figura 1A ilustra una disposición a modo de ejemplo en la que el dispositivo A, tal como un teléfono celular, PDA, ordenador portátil, y similares, incluye un transceptor de portadora de corto alcance dentro de banda tal como un transceptor de WLAN de IEEE 802.11. El dispositivo A incluye adicionalmente un transceptor de portadora de corto alcance fuera de banda, tal como un transceptor de comunicación de campo cercano (NFC).

La figura 1A ilustra adicionalmente el dispositivo B en la disposición a modo de ejemplo, tal como un teléfono celular, PDA, ordenador portátil, y similares, incluye un transceptor de portadora de corto alcance dentro de banda, tal como un transceptor de WLAN de IEEE 802.11. El dispositivo B se muestra como no estando inicialmente conectado a red WLAN alguna. El dispositivo B también incluye un transceptor de portadora de corto alcance fuera de banda, tal como un transceptor de comunicación de campo cercano (NFC).

En la figura 1B, el dispositivo A se muestra como habiéndose unido a una red WLAN al haber formado una conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 con un AP/GO de dispositivo central. El AP/GO de dispositivo central representa o bien un dispositivo de punto de acceso (AP) en una red de infraestructura o bien un dispositivo de propietario de grupo (GO) en una red P2P.

La figura 1C ilustra un ejemplo del AP/GO de dispositivo central transmitiendo la información de autenticación 25 al dispositivo A por medio de la conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11, en un instante a continuación del establecimiento de una conexión de red WLAN entre el dispositivo A y el AP/GO de dispositivo central. La información de autenticación 25 puede incluir, por ejemplo, un número aleatorio o un valor basado en cifrado de clave pública generado por el AP/GO de dispositivo central. La información de autenticación 25 es reconocible por el AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. El AP/GO puede generar números aleatorios únicos para cada cliente (para mejorar la seguridad). Este número aleatorio se puede enviar de una forma segura al cliente, tal como con WPA/WPA2 que se usa normalmente entre un AP/GO y un dispositivo de cliente. Este número aleatorio se puede actualizar periódicamente. Este número aleatorio o valor de información criptográfica se puede enviar durante la configuración de conexión, tal como se describe en la figura 1C. esta información de autenticación se puede renovar en cualquier instante posterior, por ejemplo, en una renovación periódica. Asimismo, si la información de autenticación es usada por otro dispositivo conectado a la red mediante el uso de este método de toque a cliente de NFC, entonces puede ser apropiado renovar esta información de autenticación.

La información de autenticación 25 puede incluir una contraseña de dispositivo (PIN), cifrado de clave pública,

intercambio de clave de Diffie-Hellman, o intercambio de clave simétrica de norma de cifrado avanzada (AES) como la información de autenticación, por medio de una conexión de comunicación de portadora de corto alcance dentro de banda.

La figura 1D ilustra un ejemplo de un evento de toque de NFC entre los dispositivos A y B. Al usuario del dispositivo A le gustaría incluir el dispositivo B en la red WLAN al hacer que este se conecte automáticamente con el AP/GO de dispositivo central y adquiera credenciales para el acceso de red, sin requerir que el usuario teclee en un número PIN. Para lograr esto, el usuario del dispositivo A toca el transpondedor de NFC del dispositivo A con el transpondedor de NFC del dispositivo B con el fin de iniciar un procedimiento de conmutación de transporte de portadora de corto alcance con el dispositivo B. El toque de NFC da como resultado la transmisión de señales de comunicación de portadora de corto alcance fuera de banda inalámbrica de NFC para proporcionar una conexión de comunicación de portadora de corto alcance fuera de banda de NFC con el dispositivo B.

La figura 1E ilustra un ejemplo del dispositivo B que envía una solicitud de traspaso de NFC 60 de la figura 3A, al dispositivo A. Cuando el dispositivo selector de NFC A ha establecido una comunicación de LLCP con el dispositivo solicitante de NFC B, el dispositivo solicitante B envía un mensaje de solicitud de traspaso 60, que se muestra en la figura 3A, al dispositivo A, con su solicitud de información para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central.

La figura 1F ilustra un ejemplo del dispositivo A que responde con una selección de traspaso de NFC que incluye la información de autenticación 25. El dispositivo selector de NFC A entonces responde mediante el envío al dispositivo B, de un mensaje de respuesta de selección de traspaso 61, que se muestra en la figura 3B, que incluye la información de autenticación 25 y una información de conexión, tal como la dirección de MAC 26 del AP/GO de dispositivo central, para llevar a cabo una configuración de conexión entre el dispositivo B y el AP/GO de dispositivo central.

La información de autenticación 25 es reconocible por el AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. La información de autenticación 25 puede incluir, por ejemplo, un número aleatorio o un valor basado en cifrado de clave pública que se recibió previamente como la información de autenticación desde el AP/GO de dispositivo central, por medio de la conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11.

El dispositivo A también puede enviar al dispositivo B, parámetros de conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 para la conexión al AP/GO de dispositivo central, tal como la dirección de MAC del AP/GO de dispositivo central, por medio de la conexión de comunicación de portadora de corto alcance fuera de banda de NFC. Esto posibilitará que el dispositivo B configure una conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 con el AP/GO de dispositivo central de acuerdo con los parámetros de conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11.

Después del procedimiento de toque de NFC, El dispositivo B posee la información de autenticación 25 reconocible por el AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A.

La figura 1G ilustra un ejemplo del dispositivo B que emite una trama de solicitud, por ejemplo, una trama de solicitud de sondeo 130B con un elemento de información (IE) de configuración protegida de Wi-Fi (WSC) de la figura 5A, enviando la misma al AP/GO de dispositivo central en un procedimiento de configuración protegida de Wi-Fi. El elemento de información (IE) de WSC de la figura 5A puede incluir la información de autenticación 25 reconocible por el AP/GO de dispositivo central.

La figura 1H ilustra un ejemplo del AP/GO de dispositivo central reconociendo la información de autenticación 25. La información de autenticación 25 sirve como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. El AP/GO de dispositivo central concede un acceso de red al dispositivo B. El dispositivo B se conecta con el AP/GO de dispositivo central e inicia el procedimiento de control de acceso de red basado en puerto de IEEE 802.1X para una autenticación basada en puerto. El dispositivo B ejecuta el método de EAP de la configuración simple de Wi-Fi mediante el envío de un mensaje de inicio de EAPoL al AP/GO de dispositivo central. El dispositivo B y el AP/GO de dispositivo central intercambian mensajes de protocolo de registro M1-M8 para dotar al dispositivo B de unas credenciales de red para la red. El dispositivo B se desasocia entonces y se reconecta con el AP/GO de dispositivo central, usando sus nuevas credenciales de autenticación de WLAN. La figura 5B ilustra una trama de gestión de MAC 130AP a modo de ejemplo enviada por el AP/GO de dispositivo central al dispositivo B con los mensajes M2, M4, M6 y M8 en los elementos de información de WSC 502, que se usa para ensamblar las credenciales 28 en el dispositivo B.

La figura 1I ilustra un ejemplo del dispositivo B que está ahora conectado a la red con su nueva configuración y se puede comunicar con el dispositivo A a través de la red, a través del AP/GO de dispositivo central. El dispositivo B se ha unido automáticamente a la red que ahora incluye el AP/GO de dispositivo central y ambos dispositivos de cliente, el dispositivo A y el dispositivo B, sin requerir que el usuario teclee en un número PIN.

La figura 1J ilustra el diagrama de red a modo de ejemplo de la figura 1D, de un ejemplo alternativo en el que el dispositivo A transmite al dispositivo B una solicitud de traspaso de NFC 60A, tal como se muestra en la figura 3C, que incluye la información de autenticación 25 que es reconocible por el AP/GO de dispositivo central y una información de conexión 26, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

En una realización alternativa a modo de ejemplo, el dispositivo B puede generar su propio número aleatorio como una información de autenticación 25 y enviar esta al dispositivo A por medio del procedimiento de toque de NFC. El dispositivo A transmitiría entonces el número aleatorio al AP/GO de dispositivo central por medio de la conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11, de tal modo que la información de autenticación 25 es reconocible por el AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A.

En algunas realizaciones alternativas a modo de ejemplo de la invención, los transpondedores de RFID se pueden usar en los dispositivos A y B, que pueden ser del tipo pasivo o del tipo activo. Un transpondedor de RFID pasivo no requiere fuente de alimentación interna alguna para comunicar con un lector de RFID, y solo está activo cuando el mismo se encuentra cerca de un lector de RFID que excita el transpondedor con una señal de radiofrecuencia continua a una frecuencia resonante de la antena. La pequeña corriente eléctrica inducida en la antena por la señal de radiofrecuencia continua proporciona suficiente energía para que un circuito integrado en el transpondedor se encienda y transmita una respuesta modulada, por lo general mediante la retrodispersión de la onda portadora continua desde el lector de RFID. Un transpondedor de RFID pasivo puede incluir una memoria de solo lectura grabable, eléctricamente borrable y programable (EEPROM) para almacenar datos recibidos desde el lector de RFID, que modula la onda portadora continua enviada por el lector de RFID. Por lo general, las distancias de lectura para los transpondedores de RFID pasivos varían de unos pocos centímetros a unos pocos metros, dependiendo de la radiofrecuencia y el diseño de la antena. Por el contrario, los transpondedores de RFID activos requieren una fuente de alimentación para recibir y transmitir información con un lector de RFID. El transpondedor de RFID se puede fijar a o integrar con el dispositivo inalámbrico A y B y el usuario pone el transpondedor de RFID en el dispositivo A cerca de un circuito de lector de RFID en el dispositivo B para permitir una comunicación de campo cercano entre los dispositivos. En algunas realizaciones a modo de ejemplo, ambos dispositivos A y B tienen circuitos de lector de RFID para leer señales de RFID procedentes del otro dispositivo.

La figura 2 es un diagrama de red inalámbrica de una realización a modo de ejemplo del dispositivo inalámbrico A y el dispositivo inalámbrico B. El dispositivo A y el dispositivo B están equipados, cada uno, con un transceptor de NFC fuera de banda 12A y 12B, respectivamente, usando el protocolo de comunicación de campo cercano (NFC). El dispositivo A y el dispositivo B de la figura 2 y el AP/GO de dispositivo central de la figura 4, están equipados, cada uno, con uno o más transceptores de portadora de corto alcance dentro de banda, por ejemplo, el transceptor de corto alcance dentro de banda 10A, 10B y 10C, respectivamente, que usan el protocolo de IEEE 802.11. El protocolo de NFC es fuera de banda desde el punto de vista del protocolo IEEE 802.11 de dentro de banda.

En una realización a modo de ejemplo, el dispositivo A y el dispositivo B de la figura 2 y el AP/GO de dispositivo central de la figura 4, pueden ser, cada uno, un dispositivo anfitrión que tiene una función global como una PDA, teléfono celular, ordenador portátil o de bolsillo, o similares. El dispositivo A y el dispositivo B de la figura 2 y el AP/GO de dispositivo central de la figura 4, incluyen cada uno un procesador 20 que incluye una unidad de procesamiento central de núcleo doble o de núcleo múltiple (CPU_1 y CPU_2), una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), y circuitos de interfaz para la interconexión con circuitos de anfitrión 18, tal como una radio de teléfono celular, una batería y otras fuentes de alimentación, teclado numérico, pantalla táctil, visualizador, micrófono, altavoces, auriculares, cámara u otros dispositivos de formación de imágenes, etc. en el dispositivo A y el dispositivo B. La RAM y la ROM pueden ser dispositivos de memoria extraíbles tales como tarjetas inteligentes, SIM, WIM, memorias de semiconductores tales como RAM, ROM, PROMS, dispositivos de memoria flash, etc. La MAC y PHY de IEEE 802.11 10A, 10B y 10C, proporcionan el control de acceso a medios y radio para las comunicaciones de WLAN de IEEE 802.11. El dispositivo A y el dispositivo B tienen componentes similares.

La MAC y PHY de IEEE 802.11 10A del dispositivo A de la figura 2 pueden recibir una información de autenticación 25 desde el AP/GO de dispositivo central de la figura 4 y almacenarla en memoria intermedia en una memoria intermedia de entrada/salida 15. La información de autenticación 25 puede incluir, por ejemplo, un número aleatorio o un valor basado en cifrado de clave pública. La dirección de MAC del AP/GO de dispositivo central también se puede almacenar en memoria intermedia en la memoria intermedia de entrada/salida 15 del dispositivo A.

Cada circuito de NFC 12A en el dispositivo A y el circuito de NFC 12B en el dispositivo B, que usan la norma de configuración protegida de Wi-Fi (WPS), se comunica de forma bidireccional con el otro circuito de NFC 12A o 12B por medio de una inducción de campo magnético, en donde dos antenas de cuadro se encuentran cada una dentro del campo cercano de la otra, activando de forma eficaz un contacto inalámbrico mediante la formación de un transformador de núcleo de aire. Una radio de NFC a modo de ejemplo del circuito de NFC 12A o 12B opera dentro de la banda de ISM de radiofrecuencia sin licencia de 13,56 MHz, con un ancho de banda de aproximadamente 2 MHz a lo largo de una distancia típica de unos pocos centímetros. El circuito de NFC 12A o 12B se puede fijar a o ser una parte integrante del dispositivo A y el dispositivo B y el usuario pone la radio de NFC en el dispositivo cerca del otro circuito de NFC 12A o 12 B del otro dispositivo para permitir una comunicación bidireccional de campo

cercano entre los dispositivos.

Los parámetros de IEEE 802.11 30 del dispositivo A y el dispositivo B de la figura 2 y el AP/GO de dispositivo central de la figura 4, pueden incluir la información de parámetros de LAN inalámbrica y de credenciales para el identificador de conjunto de servicios de IEEE 802.11 (SSID), autenticación y tipo de cifrado desplegados por la red inalámbrica, la clave de red secreta que una estación inalámbrica necesita para autenticarse con la red, y la dirección de MAC del dispositivo que recibe la configuración (si se desconoce, esta dirección se ajusta a todo ceros).

Las instrucciones programadas de configuración protegida de Wi-Fi se pueden almacenar en el dispositivo de memoria A, el dispositivo B y el AP/GO de dispositivo central, basándose en el documento *Wi-Fi Simple Configuration Specification*, versión 2.0, para posibilitar la configuración de una red WLAN de dispositivo a dispositivo con un segundo dispositivo inalámbrico, usando señales de comunicación de campo cercano en la configuración de conexión de dispositivo a dispositivo fuera de banda. También se incluye en el dispositivo de memoria A, el dispositivo B y el AP/GO de dispositivo central, el programa de protocolo punto a punto de Wi-Fi Direct, basándose en el documento *Wi-Fi Alliance Peer-to-Peer Specification*, para redes P2P. Las instrucciones programadas se pueden poner en práctica como soporte lógico, soporte lógico inalterable, soporte físico o cualquier combinación de los mismos.

También se incluyen en el dispositivo A y el dispositivo B las instrucciones programadas de la especificación de configuración protegida de Wi-Fi (WPS) 2.0 para NFC, incluyendo el traspaso de conexión especificado para la configuración de WLAN de Infraestructura, testigo (etiqueta) de contraseña para la configuración de WLAN de Infraestructura, y testigo (etiqueta) de configuración para la configuración de WLAN de Infraestructura. También se incluyen en la memoria del dispositivo A y el dispositivo B unas instrucciones programadas para el protocolo de traspaso de conexión de NFC, basándose en el documento *NFC Connection Handover Technical Specification*. Las instrucciones programadas se pueden poner en práctica como soporte lógico, soporte lógico inalterable, soporte físico o cualquier combinación de los mismos.

En algunas realizaciones a modo de ejemplo de la invención, el AP/GO de dispositivo central también se puede equipar con un transceptor de NFC fuera de banda y una puesta en práctica que soporta el protocolo de comunicación de campo cercano (NFC).

El MAC de IEEE 10A, 10B y 10C, parámetros de IEEE 802.11 30, el programa de configuración protegida de Wi-Fi, el programa de protocolo punto a punto de Wi-Fi Direct y el programa de traspaso de conexión de NFC se pueden materializar como lógica de programa almacenada en la RAM y/o ROM en forma de secuencias de instrucciones programadas que, cuando se ejecutan en la CPU, llevan a cabo las funciones de las realizaciones divulgadas. La lógica de programa se puede entregar a la RAM grabable, PROMS, dispositivos de memoria flash, etc. del dispositivo A, el dispositivo B y el AP/GO de dispositivo central a partir de un producto de programa informático o artículo de fabricación en forma de medios utilizables por ordenador tales como dispositivos de memoria residentes, tarjetas inteligentes u otros dispositivos de memoria extraíbles. Como alternativa, estos se pueden materializar como lógica de circuito integrado en forma de disposiciones de lógica programada o circuitos integrados para aplicaciones específicas (ASIC) de diseño personalizado. Las una o más radios de PHY en el dispositivo A, el dispositivo B y el AP/GO de dispositivo central pueden ser circuitos de transceptor separados o, como alternativa, las una o más radios pueden ser un único módulo de RF capaz de manejar uno o múltiples canales de una forma de alta velocidad, multiplexada en el tiempo y en la frecuencia en respuesta a el procesador 20. El dispositivo A, el dispositivo B y el AP/GO de dispositivo central pueden tener los mismos componentes o unos similares.

Cuando el usuario pone los dos dispositivos equipados para NFC A y B muy próximos, tal como se muestra en las figuras 1A y 1B, estos pueden establecer un enlace de comunicación de NFC basándose en la especificación de protocolo de control de enlace lógico (LLCP) del Foro NFC. En este ejemplo, la intención del usuario es hacer que el dispositivo B active un protocolo de comunicación inalámbrica diferente, tal como el protocolo de WLAN de IEEE 802.11, con el fin de posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central y se una a la red P2P o red de infraestructura existente, de la cual el dispositivo A es un miembro. El dispositivo B puede usar el protocolo de traspaso de conexión del Foro NFC para solicitar desde el dispositivo A, información para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central.

El dispositivo A se muestra en las figuras 1A y 1B iniciando un traspaso de conexión de NFC fuera de banda con el dispositivo B al transmitir, el transceptor de NFC 12A, señales de comunicación inalámbrica para proporcionar la conexión de comunicación de NFC. Cuando el dispositivo selector de NFC A ha establecido una comunicación de LLCP con el dispositivo solicitante de NFC B, el dispositivo solicitante B envía en la figura 1E, un mensaje de solicitud de traspaso 60, que se muestra en la figura 3A, al dispositivo A, con su solicitud de información para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central.

El dispositivo selector de NFC A entonces responde mediante el envío al dispositivo B en la figura 1F, de un mensaje de selección de traspaso 61, que se muestra en la figura 3B, que incluye la información de autenticación 25 y una información de conexión, tal como la dirección de MAC 26 del AP/GO de dispositivo central, para llevar a cabo una configuración de conexión entre el dispositivo B y el AP/GO de dispositivo central. El mensaje de selección de

traspaso 61 incluye la información de autenticación 25 y la dirección de MAC 26 del AP/GO de dispositivo central que se emiten a partir de la memoria intermedia de entrada/salida 15 del dispositivo A. El dispositivo B de la figura 2 puede recibir una información de autenticación 25 y una dirección de MAC 26 del AP/GO de dispositivo central, que se pueden almacenar en memoria intermedia en la memoria intermedia de entrada/salida 17 del dispositivo B.

La figura 3A es una realización a modo de ejemplo de un formato de mensaje de solicitud de traspaso de NFC 60 desde el dispositivo B al dispositivo A con una solicitud de información para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central, en el registro de NDEF, enviado por el solicitante a través del enlace de NFC, de acuerdo con una realización de la presente invención. Un nuevo registro de NDEF se añade para portar la solicitud. Los mensajes de NDEF posibilitan que un solicitante de traspaso B negocie con el selector de traspaso A a través del enlace de NFC.

El mensaje de solicitud de traspaso 60 está compuesto por un registro de solicitud de traspaso que identifica la versión de la especificación de traspaso que se esté usando, y el registro de portadora alternativo que identifica el tipo de portadora objetivo al que se dirige ese traspaso, tal como un traspaso desde el enlace de NFC a un enlace de WLAN de IEEE 802.11. el registro de solicitud de traspaso puede tener una pluralidad de registros de portadora alternativos, uno para cada una de una pluralidad de posibles portadoras objetivo. el registro de solicitud de traspaso va seguido de varios registros de NDEF. Cada registro de portadora alternativo en el registro de solicitud de traspaso incluye punteros a registros de NDEF relacionados. El primer registro de NDEF al que apunta un registro de portadora alternativo contiene una configuración de portadora que caracteriza la portadora objetivo prevista, tal como IEEE 802.11. El siguiente registro de NDEF al que apunta el registro de portadora alternativo contiene datos auxiliares asociados con la portadora objetivo prevista u otra información en relación con el traspaso a la portadora objetivo.

La figura 3B es una realización a modo de ejemplo de un mensaje de selección de traspaso de NFC 61 enviado desde el dispositivo selector A al dispositivo solicitante B. Los mensajes de selección de traspaso de NFC 61 se pueden construir de forma similar a como lo son los mensajes de solicitud de traspaso 60. Un nuevo registro de NDEF se puede añadir para portar la información adicional que es necesaria para o bien dar un acuse de recibo de la solicitud, o bien proporcionar ajustes de conectividad para el dispositivo B y la información de autenticación 25, o bien para responder con una propuesta alternativa para la conexión, enviada por el selector A a través del enlace de NFC, de acuerdo con una realización de la presente invención.

La información de autenticación 25 es reconocible por el AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. La información de autenticación 25 puede incluir, por ejemplo, un número aleatorio o un valor basado en cifrado de clave pública que fue recibido previamente por el dispositivo A como la información de autenticación 25 desde el AP/GO de dispositivo central, por medio de la conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11.

La siguiente tabla 2 muestra un registro de NDEF 24 a modo de ejemplo que incluye la información de autenticación 25 portada en el registro de NDEF del mensaje de selección de traspaso de NFC 61 de la figura 3B.

Tabla 2 - Registro de NDEF 24

Atributo	**R/O**	**Notas, Valores permitidos**
SSID	R	SSID de red.
Tipo de red	R	< información de si esta es una red de Wi-Fi Direct o Infra>
Dirección de MAC de cliente	R	Dirección de MAC del cliente <puede ser necesaria por razones de seguridad>
Dirección de MAC de AP/GO	R	Dirección de MAC del AP/GO
Canal	O	<Esto acortaría el retardo debido a que entonces no es necesario buscar el canal correcto>
<Métodos de WPS soportados mediante AP/GO>	O	<Esto es útil para optimizar la interacción necesaria del usuario en el segundo procedimiento de WPS>
<otra información de identidad de dispositivo de AP/GO>	O	<puede que al usuario le resulte difícil identificar el dispositivo correcto basándose solo en la dirección de MAC. Por lo tanto, sería útil algo más de información fácil de usar, como el tipo de dispositivo, el nombre del fabricante, un nombre de dispositivo fácil de usar, el modelo del dispositivo... Nota: Esto es un problema en especial en el método de NFC y Wi-Fi Direct. >

Atributo	R/O	Notas, Valores permitidos
<Estado de dispositivo de cliente>	O	<algún tipo de información de estado de dispositivo de cliente tocado, en la forma más simple esto podría ser meramente definir que dispositivo es 'cliente'. También podría ser útil una información más detallada>
<otra información de identidad de cliente>	O	<nombre de dispositivo, UUID (en el caso de UPnP/DLNA), dirección de IP o tal identidad del dispositivo de cliente tocado, véase *)>
<Información básica de capacidad de cliente>	O	<por ejemplo, modos de Wi-Fi soportados, capacidad de realizar otra conexión de Wi-Fi, véase **>
<otros... >	O	Se permiten múltiples atributos.

Por lo general, la operación de tocar el dispositivo A con el dispositivo B se realiza debido a un deseo de que los mismos se comuniquen. De esta manera, la dirección de MAC en el registro a modo de ejemplo es una información útil. Otra información de identidad también puede ser útil para ayudar a reducir los retardos en la configuración de conexión.

Si ambos dispositivos que se tocan conjuntamente son dispositivos de cliente de las diferentes redes, entonces la información en el registro a modo de ejemplo se puede usar para decidir cuál de los dispositivos puede tener una ruta mejor para acceder a la red de otro dispositivo, por ejemplo, en la creación de conexiones paralelas.

Puede que sea posible que ambos dispositivos que se están tocando ya sean ya miembros de la misma red. En este caso, el registro a modo de ejemplo se puede usar para detectar esa situación y los dispositivos pueden continuar usando sus conexiones actuales para la comunicación entre sí.

Por lo general, el toque de NFC es 'ciego', lo que quiere decir que no hay comunicación de WLAN dentro de banda anterior alguna entre los dispositivos tocados. Sin embargo, al menos en el caso de infraestructura, también se soporta la señalización de 'toque durante dentro de banda', pero la información para el registro de NFC puede diferir.

En el caso de toque ciego, los dispositivos que se están tocando no tienen información anterior alguna uno de otro y, por lo tanto, es necesario portar toda la información relevante a través del enlace de NFC para posibilitar una comunicación dentro de banda de WLAN adicional.

La figura 3C es una realización alternativa a modo de ejemplo de un ejemplo de un mensaje de solicitud de traspaso de NFC 60A enviado desde el dispositivo A al dispositivo B, tal como se muestra en la figura 1J, para proporcionar ajustes de conectividad 26 y la información de autenticación 25 reconocible por el AP/GO de dispositivo central, para obtener un acceso de red a través del AP/GO de dispositivo central, de acuerdo con una realización de la presente invención.

La figura 4 es un diagrama de red inalámbrica de una realización a modo de ejemplo del dispositivo B y el AP/GO de dispositivo central. El dispositivo B y el AP/GO de dispositivo central están equipados, cada uno, con uno o más transceptores de portadora de corto alcance dentro de banda, por ejemplo, el transceptor de corto alcance dentro de banda 10B y 10C, respectivamente, que usan el protocolo de IEEE 802.11. Después del procedimiento de toque de NFC, el dispositivo B posee la información de autenticación 25 reconocible por el AP/GO de dispositivo central, en su memoria intermedia de entrada/salida 17, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A.

El dispositivo B emite una trama de solicitud, por ejemplo, una trama de solicitud de sondeo 130B con un elemento de información (IE) de configuración protegida de Wi-Fi (WSC) de la figura 5A, enviando la misma al AP/GO de dispositivo central en un procedimiento de configuración protegida de Wi-Fi. El elemento de información (IE) de WSC de la figura 5A puede incluir la información de autenticación 25 reconocible por el AP/GO de dispositivo central. El elemento de información (IE) de WSC incluye la información de autenticación 25 que se emitió desde la memoria intermedia de entrada/salida 17 del dispositivo B. El AP/GO de dispositivo central de la figura 4 puede recibir una información de autenticación 25, que se puede almacenar en memoria intermedia en la memoria intermedia de entrada/salida 19 del AP/GO de dispositivo central.

El AP/GO de dispositivo central reconocerá la información de autenticación 25, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. En respuesta, el AP/GO de dispositivo central concederá un acceso de red al dispositivo B. El dispositivo B se conecta con el AP/GO de dispositivo central e inicia el procedimiento de control de acceso de red basado en puerto de IEEE 802.1X para una autenticación basada en puerto. El dispositivo B ejecuta el método de EAP de la configuración simple de Wi-Fi mediante el envío de un mensaje de inicio de EAPoL al AP/GO de dispositivo central. El dispositivo B y el AP/GO de dispositivo central intercambian mensajes de protocolo de registro M1-M8, tal como la trama 130AP de la figura 5B, para dotar al dispositivo B de unas credenciales de red 28 para la red. Un ejemplo de las credenciales 28 se muestra

en la tabla 1, anteriormente.

El dispositivo B se desasocia entonces y se reconecta con el AP/GO de dispositivo central, usando sus nuevas credenciales de autenticación de WLAN 28. El dispositivo B está ahora conectado a la red con su nueva configuración y se puede comunicar con el dispositivo A a través de la red, a través del AP/GO de dispositivo central. El dispositivo B se ha unido automáticamente a la red que ahora incluye el AP/GO de dispositivo central y ambos dispositivos de cliente, el dispositivo A y el dispositivo B, sin requerir que el usuario teclee en un número PIN.

La figura 5A ilustra una realización a modo de ejemplo de una trama de solicitud de IEEE 802.11, por ejemplo, una trama de solicitud de sondeo 130B enviada por el dispositivo B al AP/GO de dispositivo central con la información de autenticación 25 en un elemento de información (IE) de WSC 500. El AP/GO de dispositivo central responde con sus propios datos de descubrimiento en un elemento de información de WSC de respuesta de sondeo. Entonces el dispositivo B se conecta con el AP/GO de dispositivo central e inicia el procedimiento de control de acceso de red basado en puerto de IEEE 802.1X para una autenticación basada en puerto. El dispositivo B y el AP/GO de dispositivo central intercambian mensajes de protocolo de registro M1-M8, tal como la trama 130AP de la figura 5B, para dotar al dispositivo B de unas credenciales de red 28 para la red en la memoria intermedia 17 del dispositivo B.

La trama de solicitud de sondeo 130B incluye un encabezamiento de gestión de IEEE 802.11 que incluye el tipo de trama de MAC 521 que indica que esta es una trama de gestión. El campo 522 identifica la trama 130B como un paquete de solicitud de sondeo. La porción de cabida útil de la trama de solicitud de sondeo 130B incluye el elemento de información (IE) de WSC 500 que incluye un campo de ID de elemento 523 y el registro 24 con una información de autenticación 25 en el campo 526.

La figura 5B ilustra una realización a modo de ejemplo de una trama de gestión de MAC 130AP enviada por el AP/GO de dispositivo central al dispositivo B con los mensajes M2, M4, M6 y M8 en los elementos de información de WSC 502, que se usa para ensamblar las credenciales 28 en el dispositivo B. La trama de respuesta 130AP incluye un encabezamiento de gestión de IEEE 802.11 que incluye el tipo de trama de MAC 531 que indica que esta es una trama de gestión. El campo 532 identifica la trama 130AP como un paquete de respuesta de asociación. La porción de cabida útil de la trama de respuesta 130AP incluye el elemento de información (IE) de WSC 502 que incluye un campo de ID de elemento 533 y uno de los mensajes M2, M4, M6, M8 para ensamblar unas credenciales 28 en el campo 536.

La figura 6A es un diagrama de flujo 600 a modo de ejemplo de etapas operativas a modo de ejemplo de una realización a modo de ejemplo del método llevado a cabo entre los dos dispositivos inalámbricos de la figura 2, de acuerdo con una realización de la presente invención. Las etapas del diagrama de flujo representan instrucciones de código informático almacenadas en la memoria RAM y/o ROM del dispositivo inalámbrico A, que, cuando son ejecutadas por las unidades de procesamiento central (CPU), llevan a cabo las funciones de las realizaciones a modo de ejemplo de la invención. Las etapas se pueden llevar a cabo en un orden diferente al que se muestra y las etapas individuales se pueden combinar o separarse en etapas componentes. En esta secuencia se pueden incluir etapas adicionales. Las etapas del método a modo de ejemplo son tal como sigue.

Etapa 602: participar, por parte de un primer dispositivo, en una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo;
Etapa 604: intercambiar, por parte del primer dispositivo, información con un segundo dispositivo a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo la información intercambiada unos parámetros de conexión de comunicación dentro de banda para posibilitar que el segundo dispositivo se una a la red inalámbrica y una información de autenticación reconocible por el al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica;
Etapa 606: recibir, por parte del primer dispositivo, la información de autenticación desde el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo, por medio de una conexión de comunicación dentro de banda; y
Etapa 608: enviar, por parte del primer dispositivo, la información de autenticación y los parámetros de conexión de comunicación dentro de banda, al segundo dispositivo por medio de la portadora de corto alcance fuera de banda inalámbrica.

La figura 6B es un diagrama de flujo 620 a modo de ejemplo de etapas operativas a modo de ejemplo de una realización a modo de ejemplo del método llevado a cabo entre los dos dispositivos inalámbricos de la figura 2, de acuerdo con una realización de la presente invención. Las etapas del diagrama de flujo representan instrucciones de código informático almacenadas en la memoria RAM y/o ROM del dispositivo inalámbrico B, que, cuando son ejecutadas por las unidades de procesamiento central (CPU), llevan a cabo las funciones de las realizaciones a modo de ejemplo de la invención. Las etapas se pueden llevar a cabo en un orden diferente al que se muestra y las etapas individuales se pueden combinar o separarse en etapas componentes. En esta secuencia se pueden incluir etapas adicionales. Las etapas del método a modo de ejemplo son tal como sigue.

Etapa 622: intercambiar, por medio de un aparato, información con un primer dispositivo a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo la información intercambiada unos parámetros de

conexión de comunicación dentro de banda para posibilitar que el aparato se una a una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo, y una información de autenticación reconocible por el al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica;
Etapa 624: recibir, por medio del aparato, la información de autenticación y los parámetros de conexión de comunicación dentro de banda, desde el primer dispositivo por medio de la portadora de corto alcance fuera de banda inalámbrica, habiendo sido reenviada la información de autenticación por el primer dispositivo desde el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y Etapa 626: transmitir, por medio del aparato, la información de autenticación al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo por medio de una conexión de comunicación dentro de banda para posibilitar que el aparato se una a la red inalámbrica, de acuerdo con los parámetros de conexión de comunicación dentro de banda.

La figura 6C es un diagrama de flujo 680 a modo de ejemplo de etapas operativas a modo de ejemplo de una realización a modo de ejemplo del método llevado a cabo entre el dispositivo A, el dispositivo B y el AP/GO de dispositivo central de la figura 2 y la figura 4, de acuerdo con una realización de la presente invención. Las etapas del diagrama de flujo representan instrucciones de código informático almacenadas en la memoria RAM y/o ROM del AP/GO de dispositivo central, que, cuando son ejecutadas por las unidades de procesamiento central (CPU), llevan a cabo las funciones de las realizaciones a modo de ejemplo de la invención. Las etapas se pueden llevar a cabo en un orden diferente al que se muestra y las etapas individuales se pueden combinar o separarse en etapas componentes. En esta secuencia se pueden incluir etapas adicionales. Las etapas del método a modo de ejemplo son tal como sigue.

Etapa 682: transmitir, por medio de un aparato, una información de autenticación, a un primer dispositivo inalámbrico por medio de una conexión de comunicación dentro de banda, para posibilitar que el primer dispositivo transfiera a un segundo dispositivo inalámbrico la información de autenticación por medio de una conexión de comunicación de portadora de corto alcance fuera de banda con el segundo dispositivo;
Etapa 684: recibir, por medio del aparato, la información de autenticación, desde el segundo dispositivo inalámbrico, por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda; y
Etapa 686: conceder, por medio del aparato, acceso al segundo dispositivo para unirse a una red inalámbrica por medio de la segunda conexión de comunicación dentro de banda, si la información de autenticación recibida se corresponde con la información de autenticación transmitida.

La figura 7 es un diagrama de secuencia a modo de ejemplo de un ejemplo de realización que muestra la interacción del dispositivo A, el dispositivo B y el AP/GO de dispositivo central de la figura 1B, de acuerdo con una realización de la presente invención. En el instante T1, el AP/GO de dispositivo central transmite la información de autenticación 25 al dispositivo A por medio de la conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11. En el instante T2, el usuario del dispositivo A toca el transpondedor de NFC del dispositivo A con el transpondedor de NFC del dispositivo B, dando como resultado una conexión de comunicación de portadora de corto alcance fuera de banda de NFC. En el instante T3, el dispositivo A envía una información de autenticación 25 al dispositivo B por medio de la conexión de comunicación de portadora de corto alcance fuera de banda inalámbrica de NFC. En el instante T4, el dispositivo B emite una trama de solicitud, por ejemplo, una trama de solicitud de sondeo con la información de autenticación 25 al AP/GO de dispositivo central. En el instante T5, el AP/GO de dispositivo central reconoce la información de autenticación 25 y concede un acceso de red al dispositivo B.

En algunas realizaciones de la invención, el dispositivo A puede enviar alguna información no segura (dirección de MAC del AP/GO, nombre de red, canal, etc). Además de esto, la información de autenticación 25 se envía como una información de 'prueba de toque' a través del enlace de NFC. Las alternativas a modo de ejemplo para la información de autenticación 25 incluyen:

1) número aleatorio

a) El dispositivo B genera un número, y este se pasa a través de NFC al dispositivo A y, entonces, al AP/GO

b) El AP/GO genera un número, y este se reenvía al dispositivo A y, entonces, se pasa a través de NFC al dispositivo B (Nota: Puede que el dispositivo A necesite tener este número por adelantado debido a que podría no haber suficiente tiempo para consultar el mismo al AP/GO durante el toque.

2) Prueba basada en clave pública; diversos métodos posibles, pero podría no ser factible el envío de una clave pública real a través de NFC (podría ser demasiado larga para llevarla a través de NFC).
3) Cualquier otra información única proporcionada por otros métodos criptográficos disponibles solo a través de la interfaz de NFC, es decir, esta información no se puede adquirir meramente escuchando la información de Wi-Fi enviada por AP/GO. Otros métodos criptográficos para la generación de la información de autenticación 25 para pasar a través de la interfaz de NFC pueden incluir generar una contraseña de dispositivo (PIN), un intercambio de clave de Diffie-Hellman de 1536 bits, o un intercambio de clave simétrica de norma de cifrado avanzada (AES) de 128 bits.

4) Se pueden usar claves de red temporales, en las que AP/GO da una clave temporal que es válida solo un cierto tiempo (por ejemplo, una sesión de Wi-Fi), por lo tanto, el permiso de acceso de red solo es temporal.

En el caso P2P de Wi-Fi Direct, algunas realizaciones de la invención proporcionan beneficios adicionales, debido a que, por lo general, el usuario no sabe cuál de los dispositivos es el propietario de grupo P2P, en especial en los métodos de NFC y de botón pulsador (PBC). En el caso del PIN, solo los propietarios de grupo (GO) se mostrarían al usuario y, por lo tanto, no debería ser un problema la selección accidental de un dispositivo de cliente.

En algunas realizaciones alternativas a modo de ejemplo, tal como se muestra en las figuras 8A a 8H, la información de autenticación 25 para la información de 'prueba de toque' puede ser generada por el dispositivo B y enviarse a través del enlace de NFC al dispositivo A. Por ejemplo, un número aleatorio puede ser generado por el dispositivo B y este se pasa a través del enlace de NFC por medio del procedimiento de toque de NFC al dispositivo A y, entonces, el dispositivo A transmite el número aleatorio al AP/GO de dispositivo central. El dispositivo A transmite el número aleatorio al AP/GO de dispositivo central por medio de la conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11, de tal modo que la información de autenticación 25 es reconocible por el AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A.

En la figura 8A, el dispositivo A se muestra como habiéndose unido a una red WLAN al haber formado una conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 con un AP/GO de dispositivo central. El AP/GO de dispositivo central representa o bien un dispositivo de punto de acceso (AP) en una red de infraestructura o bien un dispositivo de propietario de grupo (GO) en una red P2P. El dispositivo B se muestra habiendo generado la información de autenticación 25 en cualquier momento antes o después del establecimiento de una conexión de red WLAN entre el dispositivo A y el AP/GO de dispositivo central. La información de autenticación 25 puede incluir, por ejemplo, un número aleatorio o un valor basado en cifrado de clave pública generado por el dispositivo B. Este número aleatorio se puede actualizar periódicamente.

La figura 8B ilustra un evento de toque de NFC entre los dispositivos A y B. Al usuario del dispositivo A le gustaría incluir el dispositivo B en la red WLAN al hacer que este se conecte automáticamente con el AP/GO de dispositivo central y adquiera credenciales para el acceso de red, sin requerir que el usuario teclee en un número PIN. Para lograr esto, el usuario del dispositivo A toca el transpondedor de NFC del dispositivo A con el transpondedor de NFC del dispositivo B con el fin de iniciar un procedimiento de conmutación de transporte de portadora de corto alcance con el dispositivo B. El toque de NFC da como resultado la transmisión de señales de comunicación de portadora de corto alcance fuera de banda inalámbrica de NFC para proporcionar una conexión de comunicación de portadora de corto alcance fuera de banda de NFC con el dispositivo B.

La figura 8C ilustra un dispositivo B a modo de ejemplo que envía una solicitud de traspaso de NFC al dispositivo A que incluye una información de autenticación 25. Cuando el dispositivo selector de NFC A ha establecido una comunicación de LLCP con el dispositivo solicitante de NFC B, el dispositivo solicitante B envía un mensaje de solicitud de traspaso 60', que se muestra en la figura 9A, al dispositivo A, con su solicitud de información para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central. El mensaje de solicitud de traspaso de NFC 60' incluye un registro de NDEF 24 con la información de autenticación 25.

La figura 8D ilustra un dispositivo A a modo de ejemplo que responde con una selección de traspaso de NFC que incluye la información de conectividad 26, tal como la dirección de MAC para el AP/GO de dispositivo central. El dispositivo selector de NFC A responde mediante el envío al dispositivo B, de un mensaje de respuesta de selección de traspaso 61', que se muestra en la figura 9B, que incluye la información de conectividad 26, para llevar a cabo una configuración de conexión entre el dispositivo B y el AP/GO de dispositivo central.

El dispositivo A envía al dispositivo B, parámetros de conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 para la conexión al AP/GO de dispositivo central, tal como la dirección de MAC del AP/GO de dispositivo central, por medio de la conexión de comunicación de portadora de corto alcance fuera de banda de NFC. Esto posibilitará que el dispositivo B configure una conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11 con el AP/GO de dispositivo central de acuerdo con los parámetros de conexión de comunicación de portadora de corto alcance dentro de banda de IEEE 802.11.

Después del procedimiento de toque de NFC, el dispositivo A posee la información de autenticación 25 reconocible por el AP/GO de dispositivo central, que servirá como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A.
La figura 8E ilustra un dispositivo A a modo de ejemplo que envía una trama de gestión 130A con un elemento de información (IE) de configuración protegida de Wi-Fi (WSC) de la figura 10, enviando la misma al AP/GO de dispositivo central en un procedimiento de configuración protegida de Wi-Fi. El elemento de información (IE) de WSC 504 de la figura 10 incluye la información de autenticación 25 reconocible por el AP/GO de dispositivo central.

La figura 8F ilustra un dispositivo B a modo de ejemplo que emite una trama de solicitud, por ejemplo, una trama de

solicitud de sondeo 130B con un elemento de información (IE) de configuración protegida de Wi-Fi (WSC) de la figura 5A, enviando la misma al AP/GO de dispositivo central en un procedimiento de configuración protegida de Wi-Fi. El elemento de información (IE) de WSC 500 de la figura 5A incluye la información de autenticación 25 reconocible por el AP/GO de dispositivo central.

La figura 8G ilustra el AP/GO de dispositivo central reconociendo la información de autenticación 25. La información de autenticación 25 sirve como una prueba de que el dispositivo B sí entró en contacto, de hecho, en un toque de NFC con el dispositivo A. El AP/GO de dispositivo central concede un acceso de red al dispositivo B. El dispositivo B se conecta con el AP/GO de dispositivo central e inicia el procedimiento de control de acceso de red basado en puerto de IEEE 802.1X para una autenticación basada en puerto. El dispositivo B ejecuta el método de EAP de la configuración simple de Wi-Fi mediante el envío de un mensaje de inicio de EAPoL al AP/GO de dispositivo central. El dispositivo B y el AP/GO de dispositivo central intercambian mensajes de protocolo de registro M1-M8 para dotar al dispositivo B de unas credenciales de red para la red. El dispositivo B se desasocia entonces y se reconecta con el AP/GO de dispositivo central, usando sus nuevas credenciales de autenticación de WLAN. La figura 5B ilustra una trama de gestión de MAC 130AP a modo de ejemplo enviada por el AP/GO de dispositivo central al dispositivo B con los mensajes M2, M4, M6 y M8 en los elementos de información de WSC 502, que se usa para ensamblar las credenciales 28 en el dispositivo B.

La figura 8H ilustra que el dispositivo B está ahora conectado a la red con su nueva configuración y se puede comunicar con el dispositivo A a través de la red, a través del AP/GO de dispositivo central. El dispositivo B se ha unido automáticamente a la red que ahora incluye el AP/GO de dispositivo central y ambos dispositivos de cliente, el dispositivo A y el dispositivo B, sin requerir que el usuario teclee en un número PIN.

La figura 8I ilustra el diagrama de red a modo de ejemplo de la figura 8B, de un ejemplo alternativo en el que el dispositivo A transmite una solicitud de traspaso de NFC 60B, que se muestra en la figura 9C, que incluye una información de conexión 26, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 8J ilustra el diagrama de red a modo de ejemplo de la figura 8I, de un ejemplo alternativo en el que el dispositivo B está respondiendo con una selección de traspaso de NFC 61B, que se muestra en la figura 9D, al dispositivo A, que incluye una información de autenticación 25, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 9C es una realización alternativa a modo de ejemplo de un mensaje de solicitud de traspaso de NFC 60B enviado desde el dispositivo A al dispositivo B en la figura 8I, para proporcionar ajustes de conectividad 26 para obtener un acceso de red a través del AP/GO de dispositivo central, de acuerdo con una realización de la presente invención.

La figura 9D es una realización alternativa a modo de ejemplo de un mensaje de selección de traspaso de NFC 61B enviado desde el dispositivo B al dispositivo A en la figura 8J, que incluye la información de autenticación 25, para posibilitar que el dispositivo B obtenga un acceso de red a través del AP/GO de dispositivo central, de acuerdo con algunas realizaciones a modo de ejemplo de la invención.

La figura 11A es un diagrama de flujo 1100 a modo de ejemplo de etapas operativas a modo de ejemplo de una realización a modo de ejemplo del método llevado a cabo entre los dos dispositivos inalámbricos de la figura 2 y las figuras 8A - 8H, de acuerdo con una realización de la presente invención. Las etapas del diagrama de flujo representan instrucciones de código informático almacenadas en la memoria RAM y/o ROM del dispositivo inalámbrico A, que, cuando son ejecutadas por las unidades de procesamiento central (CPU), llevan a cabo las funciones de las realizaciones a modo de ejemplo de la invención. Las etapas se pueden llevar a cabo en un orden diferente al que se muestra y las etapas individuales se pueden combinar o separarse en etapas componentes. En esta secuencia se pueden incluir etapas adicionales. Las etapas del método a modo de ejemplo son tal como sigue.

Etapa 1102: participar, por parte de un primer dispositivo, en una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo;
Etapa 1104: intercambiar, por parte del primer dispositivo, información con un segundo dispositivo a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo la información intercambiada unos parámetros de conexión de comunicación dentro de banda para posibilitar que el segundo dispositivo se una a la red inalámbrica y una información de autenticación reconocible por el al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica;
Etapa 1106: recibir, por parte del primer dispositivo, desde el segundo dispositivo, la información de autenticación por medio de la portadora de corto alcance fuera de banda inalámbrica, para su reenvío al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y
Etapa 1108: enviar, por parte del primer dispositivo, al segundo dispositivo los parámetros de conexión de comunicación dentro de banda por medio de la portadora de corto alcance fuera de banda inalámbrica, para la conexión al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo.

La figura 11B es un diagrama de flujo 1120 a modo de ejemplo de etapas operativas a modo de ejemplo de una

realización a modo de ejemplo del método llevado a cabo entre los dos dispositivos inalámbricos de la figura 2 y las figuras 8A - 8H, de acuerdo con una realización de la presente invención. Las etapas del diagrama de flujo representan instrucciones de código informático almacenadas en la memoria RAM y/o ROM del dispositivo inalámbrico B, que, cuando son ejecutadas por las unidades de procesamiento central (CPU), llevan a cabo las funciones de las realizaciones a modo de ejemplo de la invención. Las etapas se pueden llevar a cabo en un orden diferente al que se muestra y las etapas individuales se pueden combinar o separarse en etapas componentes. En esta secuencia se pueden incluir etapas adicionales. Las etapas del método a modo de ejemplo son tal como sigue.

Etapa 1122: intercambiar, por medio de un aparato, información con un primer dispositivo a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo la información intercambiada unos parámetros de conexión de comunicación dentro de banda para posibilitar que el aparato se una a una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo, y una información de autenticación reconocible por el al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica;
Etapa 1124: enviar, por medio del aparato, al primer dispositivo, la información de autenticación por medio de la portadora de corto alcance fuera de banda inalámbrica, para su reenvío al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y
Etapa 1126: recibir, por medio del aparato, desde el primer dispositivo, los parámetros de conexión de comunicación dentro de banda por medio de la portadora de corto alcance fuera de banda inalámbrica, para la conexión al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo.

La figura 11C es un diagrama de flujo 1130 a modo de ejemplo de etapas operativas a modo de ejemplo de una realización a modo de ejemplo del método llevado a cabo entre el dispositivo A, el dispositivo B y el AP/GO de dispositivo central de la figura 2 y la figura 4 y las figuras 8A - 8H, de acuerdo con una realización de la presente invención. Las etapas del diagrama de flujo representan instrucciones de código informático almacenadas en la memoria RAM y/o ROM del AP/GO de dispositivo central, que, cuando son ejecutadas por las unidades de procesamiento central (CPU), llevan a cabo las funciones de las realizaciones a modo de ejemplo de la invención. Las etapas se pueden llevar a cabo en un orden diferente al que se muestra y las etapas individuales se pueden combinar o separarse en etapas componentes. En esta secuencia se pueden incluir etapas adicionales. Las etapas del método a modo de ejemplo son tal como sigue.

Etapa 1132: recibir, por medio de un aparato, una información de autenticación desde un primer dispositivo inalámbrico por medio de una conexión de comunicación de portadora de corto alcance dentro de banda;
Etapa 1134: recibir, por medio del aparato, la información de autenticación desde el segundo dispositivo inalámbrico por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda; y
Etapa 1136: conceder, por medio del aparato, acceso al segundo dispositivo para unirse a una red inalámbrica por medio de la segunda conexión de comunicación de portadora de corto alcance dentro de banda si la información de autenticación recibida desde el segundo dispositivo inalámbrico se corresponde con la información de autenticación recibida desde el primer dispositivo inalámbrico.

En una realización a modo de ejemplo, el un transceptor de portadora de corto alcance fuera de banda en el dispositivo A y el dispositivo B puede ser un protocolo de comunicaciones de corto alcance adecuado, tal como identificación por radiofrecuencia (RFID), comunicación de campo cercano (NFC), asociación de datos infrarrojos (IrDA) o banda ultraancha (UWB), por ejemplo.

Un ejemplo de la portadora de corto alcance fuera de banda de identificación por radiofrecuencia (RFID) se describe, por ejemplo, en la norma ISO 11785 (protocolo de interfaz aérea), la norma ISO 14443 (protocolo de interfaz aérea) y la norma ISO 15693.

Un ejemplo de la portadora de corto alcance fuera de banda de comunicación de campo cercano (NFC) se describe, por ejemplo, en la norma ISO/IEC 14443 y la norma ISO/IEC 18092.

Un ejemplo de la portadora de corto alcance fuera de banda de la asociación de datos infrarrojos (IrDA) se describe, por ejemplo, en el Protocolo de acceso de enlace de IrDA, v1.1 (1996).

Un ejemplo de la portadora de corto alcance fuera de banda de banda ultraancha (UWB) se describe, por ejemplo, en el documento *WiMedia Common Radio Platform Specification*, versión 1.5 (2010).

En algunas realizaciones a modo de ejemplo, el transceptor de portadora de corto alcance dentro de banda en el dispositivo A, el dispositivo B y el AP/GO de dispositivo central puede ser un protocolo de comunicaciones adecuado, tal como un protocolo de comunicaciones de área de vehículos (WEAN), un protocolo de comunicaciones de redes de vídeo inalámbrico (WVAN-TV), un protocolo de comunicaciones de área personal (WPAN), un protocolo de comunicaciones de área local (WLAN) o un protocolo de comunicaciones de área extensa (WAN), usando los procedimientos y primitivas convencionales definidos por las normas respectivas. Los protocolos de comunicaciones de área personal (WPAN) incluyen BR/EDR de Bluetooth, Baja Energía de Bluetooth, USB inalámbrico (WUSB), banda ultraancha (UWB), ZigBee (IEEE 802.15.4 o IEEE 802.15.4a) para una comunicación de corto alcance entre

dispositivos. Los protocolos de comunicaciones de área local (WLAN) incluyen telecomunicaciones digitales potenciadas sin hilos (DECT) e HIPERLAN. Los protocolos de comunicaciones de área extensa (WAN) incluyen sistema global para comunicaciones móviles (GSM), servicio de radio general por paquetes (GPRS), tasas de datos potenciadas para evolución de GSM (EDGE), datos de evolución optimizados (EV-DO) y acceso múltiple por división de código de banda ancha (WCDMA).

Usando la descripción proporcionada en el presente documento, las realizaciones se pueden poner en práctica como una máquina, un proceso o un artículo de fabricación mediante el uso de técnicas de programación y/o de diseño convencionales para producir soporte lógico de programación, soporte lógico inalterable, soporte físico o cualquier combinación de los mismos.

Cualquier programa o programas resultantes, que tenga código de programa legible por ordenador, se pueden materializar en uno o más medios utilizables por ordenador tales como dispositivos de memoria residentes, tarjetas inteligentes u otros dispositivos de memoria extraíbles, o dispositivos de transmisión, haciendo de ese modo un producto de programa informático o artículo de fabricación de acuerdo con las realizaciones. En ese sentido, las expresiones "artículo de fabricación" y "producto de programa informático" tal como se usan en el presente documento tienen por objeto abarcar un programa informático que exista de forma permanente o temporal en cualquier medio utilizable por ordenador o en cualquier medio de transmisión que transmita un programa de ese tipo.

Tal como se ha indicado en lo que antecede, los dispositivos de memoria/almacenamiento incluyen, pero no se limitan a, discos, discos ópticos, dispositivos de memoria extraíbles tales como tarjetas inteligentes, SIM, WIM, memorias de semiconductores tales como RAM, ROM, PROMS, etc. Los medios de transmisión incluyen, pero no se limitan a, transmisiones por medio de redes de comunicación inalámbrica, Internet, intranets, comunicación de red basada en teléfono/módem, red de comunicación por cable/cableada, comunicación por satélite, y otros sistemas de red/enlaces de comunicación estacionarios o móviles.

Aunque se han divulgado realizaciones específicas a modo de ejemplo, un experto en la materia entenderá que se pueden realizar cambios en las realizaciones específicas a modo de ejemplo sin apartarse del alcance de la invención.

REIVINDICACIONES

1. Un método, en un primer dispositivo, que comprende:

participar (1102), por parte del primer dispositivo, en una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo;
intercambiar (1104), por parte del primer dispositivo, información con un segundo dispositivo que no está conectado con la red inalámbrica, a través de la portadora de corto alcance fuera de banda inalámbrica, comprendiendo el intercambio de información:

recibir (1106), desde el segundo dispositivo, una información de autenticación (25) por medio de una portadora de corto alcance fuera de banda inalámbrica, para su reenvío al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y enviar (1108), al segundo dispositivo, unos parámetros de conexión de comunicación dentro de banda (26) por medio de la portadora de corto alcance fuera de banda inalámbrica, para la conexión a la red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

transmitir, la información de autenticación recibida (25), al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo, por medio de una conexión de comunicación de portadora de corto alcance dentro de banda de la red inalámbrica, para posibilitar que el al menos uno del punto de acceso o el dispositivo de propietario de grupo conceda acceso al segundo dispositivo para unirse a la red inalámbrica si la información de autenticación recibida desde el primer dispositivo se corresponde con una segunda información de autenticación recibida desde el segundo dispositivo por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda.

2. El método de la reivindicación 1, en el que la portadora de corto alcance fuera de banda inalámbrica comprende una de portadora de comunicación de campo cercano o de identificación por radiofrecuencia.

3. El método de la reivindicación 1 o la reivindicación 2, en el que la conexión de comunicación de portadora de corto alcance dentro de banda comprende una de conexión de red de área local inalámbrica (WLAN) o de Bluetooth.

4. Un método, en un segundo dispositivo, que comprende:

intercambiar (1122), por parte del segundo dispositivo que no está conectado a una red inalámbrica, información con un primer dispositivo, a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo la información intercambiada:

transmitir (1124), por parte del segundo dispositivo, al primer dispositivo, una información de autenticación (25) reconocible por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica; y
recibir (1126), por parte del segundo dispositivo, desde el primer dispositivo, unos parámetros de conexión de comunicación dentro de banda (26) para habilitar al segundo dispositivo para la conexión a la red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

transmitir (1134), por parte del segundo dispositivo, la información de autenticación (25) al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo por medio de una conexión de comunicación de portadora de corto alcance dentro de banda de la red inalámbrica, de acuerdo con los parámetros de conexión de comunicación dentro de banda (26), para posibilitar que el al menos uno del punto de acceso o el dispositivo de propietario de grupo conceda acceso al segundo dispositivo para unirse a la red inalámbrica si la información de autenticación recibida desde el segundo dispositivo se corresponde con una primera información de autenticación recibida desde el primer dispositivo por medio de una primera conexión de comunicación de portadora de corto alcance dentro de banda.

5. El método de la reivindicación 4, que comprende adicionalmente:

recibir (1136), por parte del segundo dispositivo, una concesión de acceso para unirse a la red inalámbrica por medio de la conexión de comunicación de corto alcance dentro de banda desde el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo.

6. El método de la reivindicación 4 o la reivindicación 5, en el que la portadora de corto alcance fuera de banda inalámbrica comprende una de portadora de comunicación de campo cercano o de identificación por radiofrecuencia.

7. El método de cualquiera de las reivindicaciones 4-6, en el que la conexión de comunicación de portadora de corto alcance dentro de banda comprende una de conexión de red de área local inalámbrica (WLAN) o de Bluetooth.

8. Un método, en un dispositivo de punto de acceso o un dispositivo de propietario de grupo, que comprende:

recibir (1132), por parte del dispositivo de punto de acceso o el dispositivo de propietario de grupo, una primera información de autenticación (25) desde un primer dispositivo inalámbrico conectado a una red inalámbrica por medio de una conexión de comunicación dentro de banda, en donde dicha primera información de autenticación es adquirida por el primer dispositivo de acuerdo con el método de la reivindicación 1; recibir (1134), por parte del dispositivo de punto de acceso o el dispositivo de propietario de grupo, una segunda información de autenticación (25), desde el segundo dispositivo inalámbrico, por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda; y
conceder (1136), por parte del dispositivo de punto de acceso o el dispositivo de propietario de grupo, acceso al segundo dispositivo para unirse a la red inalámbrica por medio de la segunda conexión de comunicación dentro de banda, si se corresponden la primera y la segunda información de autenticación recibidas.

9. Un programa informático que comprende código de programa legible por ordenador configurado para dar lugar a la realización del método de cualquiera de las reivindicaciones anteriores cuando dicho programa se está ejecutando en un ordenador.

10. El programa informático de la reivindicación 9, en donde el programa informático es un producto de programa informático que comprende un medio legible por ordenador que porta código de programa informático materializado en el mismo para su uso con un ordenador.

11. Un aparato, que comprende:

unos medios (10A) para participar en una red inalámbrica gestionada por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo;
unos medios (12A) para intercambiar información con un segundo dispositivo que no está conectado a la red inalámbrica a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo los medios para intercambiar información:

unos medios para recibir, desde el segundo dispositivo, una información de autenticación (25) por medio de la portadora de corto alcance fuera de banda inalámbrica para su reenvío al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo;
unos medios para enviar, al segundo dispositivo, unos parámetros de conexión de comunicación dentro de banda (26) por medio de la portadora de corto alcance fuera de banda inalámbrica, para la conexión a la red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

unos medios (10A) para transmitir, la información de autenticación recibida (25), al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo, por medio de una conexión de comunicación de portadora de corto alcance dentro de banda de la red inalámbrica, para posibilitar que el al menos uno del punto de acceso o el dispositivo de propietario de grupo conceda acceso al segundo dispositivo para unirse a la red inalámbrica si la información de autenticación recibida desde el primer dispositivo se corresponde con una segunda información de autenticación recibida desde el segundo dispositivo por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda.

12. El aparato de la reivindicación 11, en el que la portadora de corto alcance fuera de banda inalámbrica comprende una de portadora de comunicación de campo cercano o de identificación por radiofrecuencia.

13. El aparato de la reivindicación 11, en el que la conexión de comunicación de portadora de corto alcance dentro de banda comprende una de conexión de red de área local inalámbrica (WLAN) o de Bluetooth.

14. Un aparato para unirse a una red inalámbrica, que comprende:

unos medios (12B) para intercambiar información con un primer dispositivo a través de una portadora de corto alcance fuera de banda inalámbrica, comprendiendo los medios para intercambiar información:

unos medios para transmitir, al primer dispositivo, una información de autenticación (25) reconocible por al menos uno de un dispositivo de punto de acceso o un dispositivo de propietario de grupo que gestiona la red inalámbrica; y
unos medios para recibir, desde el primer dispositivo, unos parámetros de conexión de comunicación dentro de banda (26) para posibilitar que el aparato se conecte a una red inalámbrica gestionada por el al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo; y

unos medios (10B) para transmitir la información de autenticación (25) al al menos uno del dispositivo de punto de acceso o el dispositivo de propietario de grupo por medio de una conexión de comunicación de portadora de corto alcance dentro de banda, de acuerdo con los parámetros de conexión de comunicación dentro de banda

(26), para posibilitar que el al menos uno del punto de acceso o el dispositivo de propietario de grupo conceda acceso al segundo dispositivo para unirse a la red inalámbrica si la información de autenticación recibida desde el segundo dispositivo se corresponde con una primera información de autenticación recibida desde el primer dispositivo por medio de una primera conexión de comunicación de portadora de corto alcance dentro de banda.

15. Un dispositivo de punto de acceso o un aparato de propietario de grupo para una red inalámbrica, que comprende:

unos medios (10AP) para recibir una primera información de autenticación (25), desde un primer dispositivo inalámbrico conectado a una red inalámbrica por medio de una conexión de comunicación dentro de banda, en donde dicha primera información de autenticación es adquirida por el primer dispositivo de acuerdo con el método de la reivindicación 1; unos medios (10AP) para recibir una segunda información de autenticación (25), desde un segundo dispositivo inalámbrico, por medio de una segunda conexión de comunicación de portadora de corto alcance dentro de banda; y
unos medios (20) para conceder acceso al segundo dispositivo para unirse a la red inalámbrica por medio de la segunda conexión de comunicación dentro de banda, si se corresponden la primera y la segunda información de autenticación recibidas.

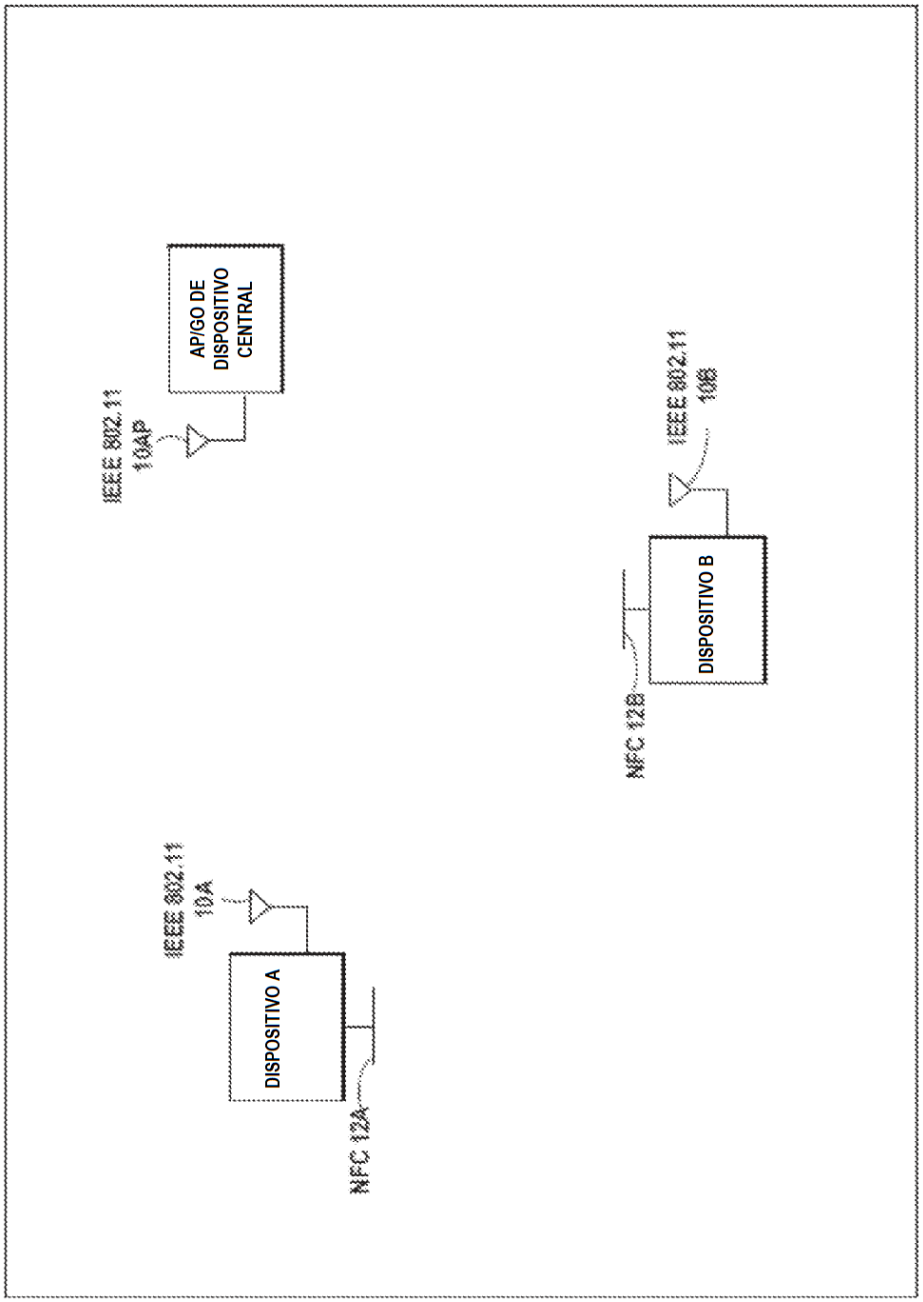

IEEE 802.11
10AP
AP/GO DE
DISPOSITIVO
CENTRAL
IEEE 802.11
10A
DISPOSITIVO A
NFC 12A
IEEE 802.11
10B
DISPOSITIVO B
NFC 12B

FIG. 1A

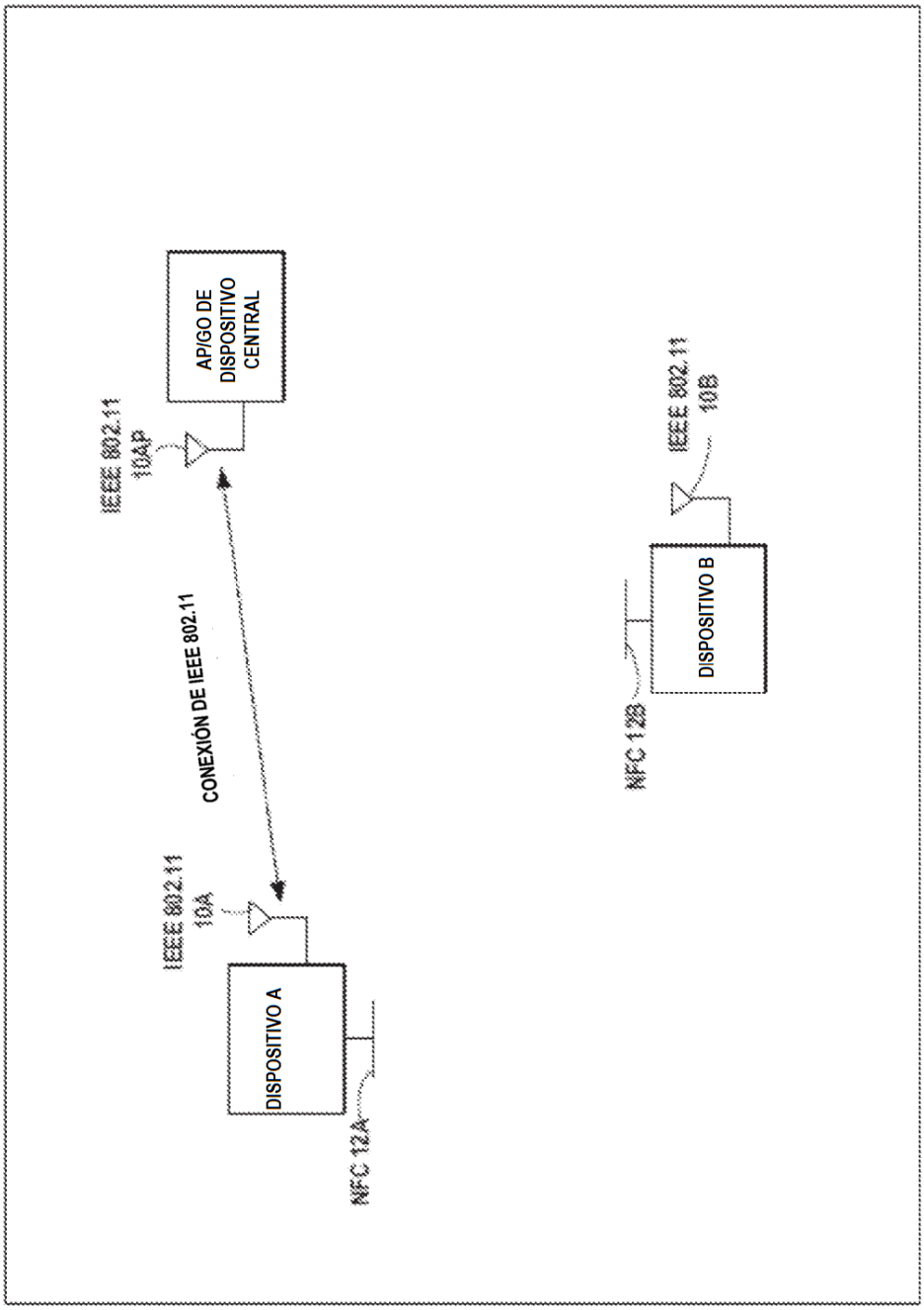

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A
NFC 12A
IEEE 802.11 10B
DISPOSITIVO B
NFC 12B

FIG. 1B

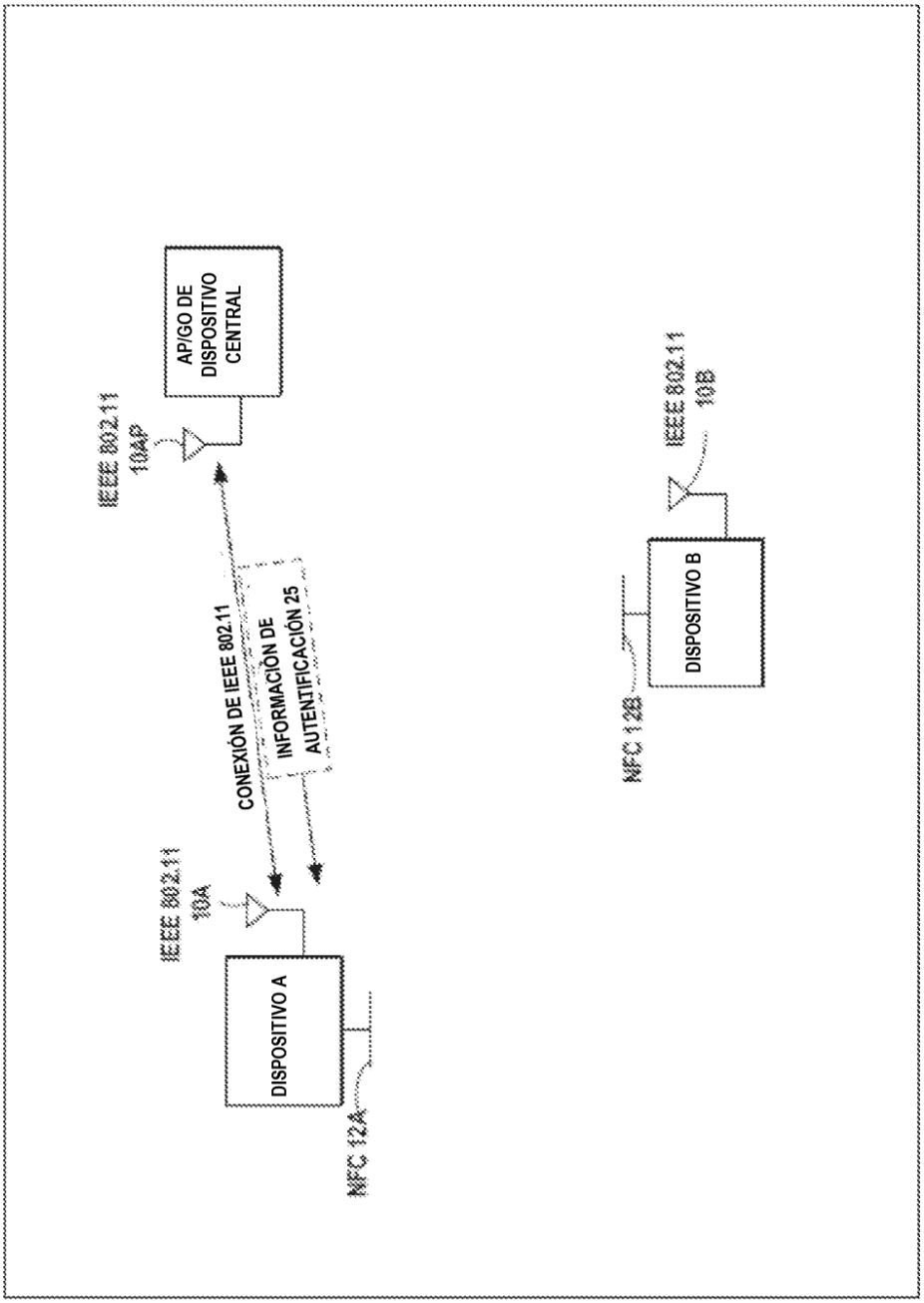

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
INFORMACIÓN DE AUTENTIFICACIÓN 25
IEEE 802.11 10A
DISPOSITIVO A
NFC 12A
IEEE 802.11 10B
DISPOSITIVO B
NFC 12B

FIG. 1C

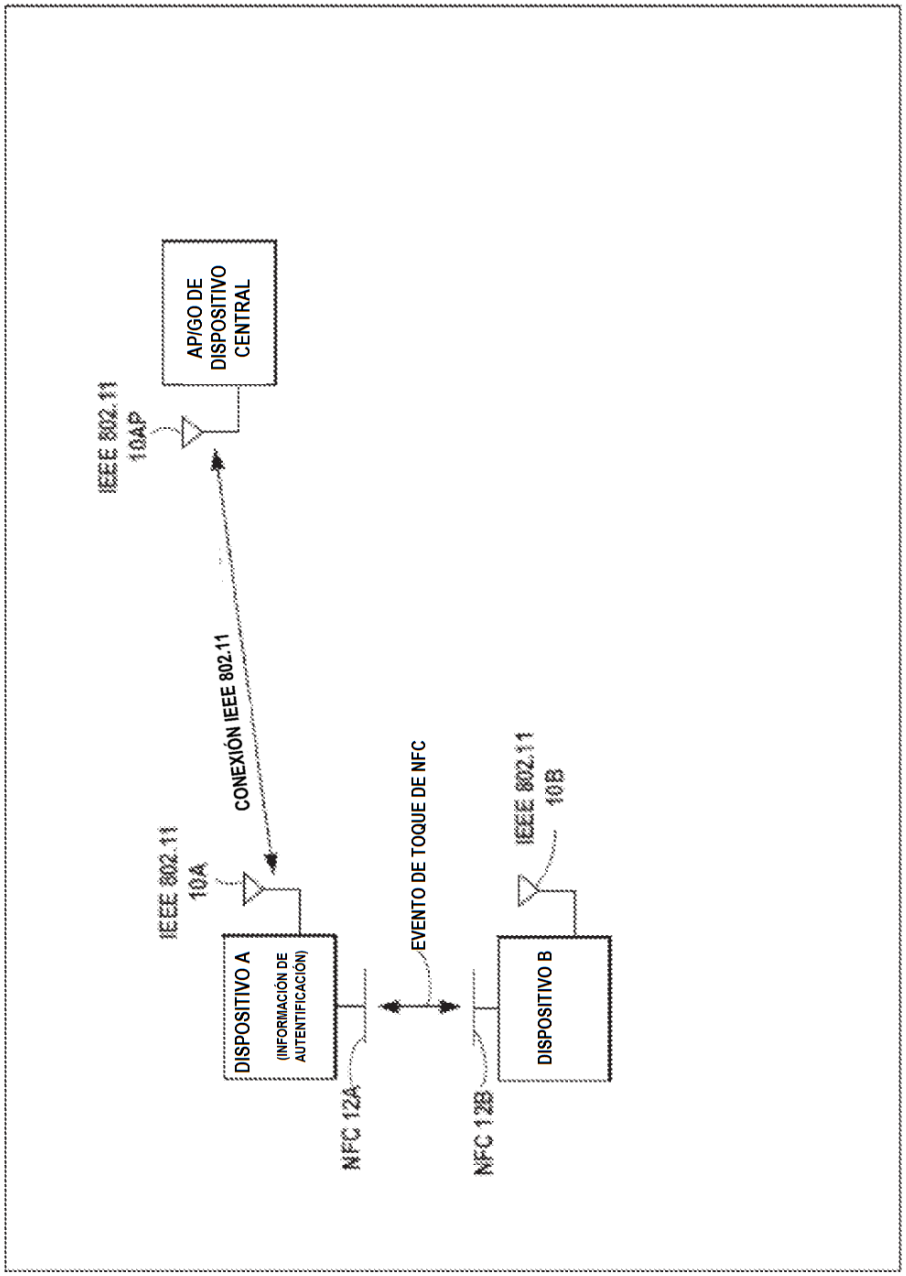

IEEE 802.11
10AP
AP/GO DE
DISPOSITIVO
CENTRAL
CONEXIÓN IEEE 802-11
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12A
EVENTO DE TOQUE DE NFC
NFC 12B
IEEE 802.11
10B
DISPOSITIVO B

FIG. 1D

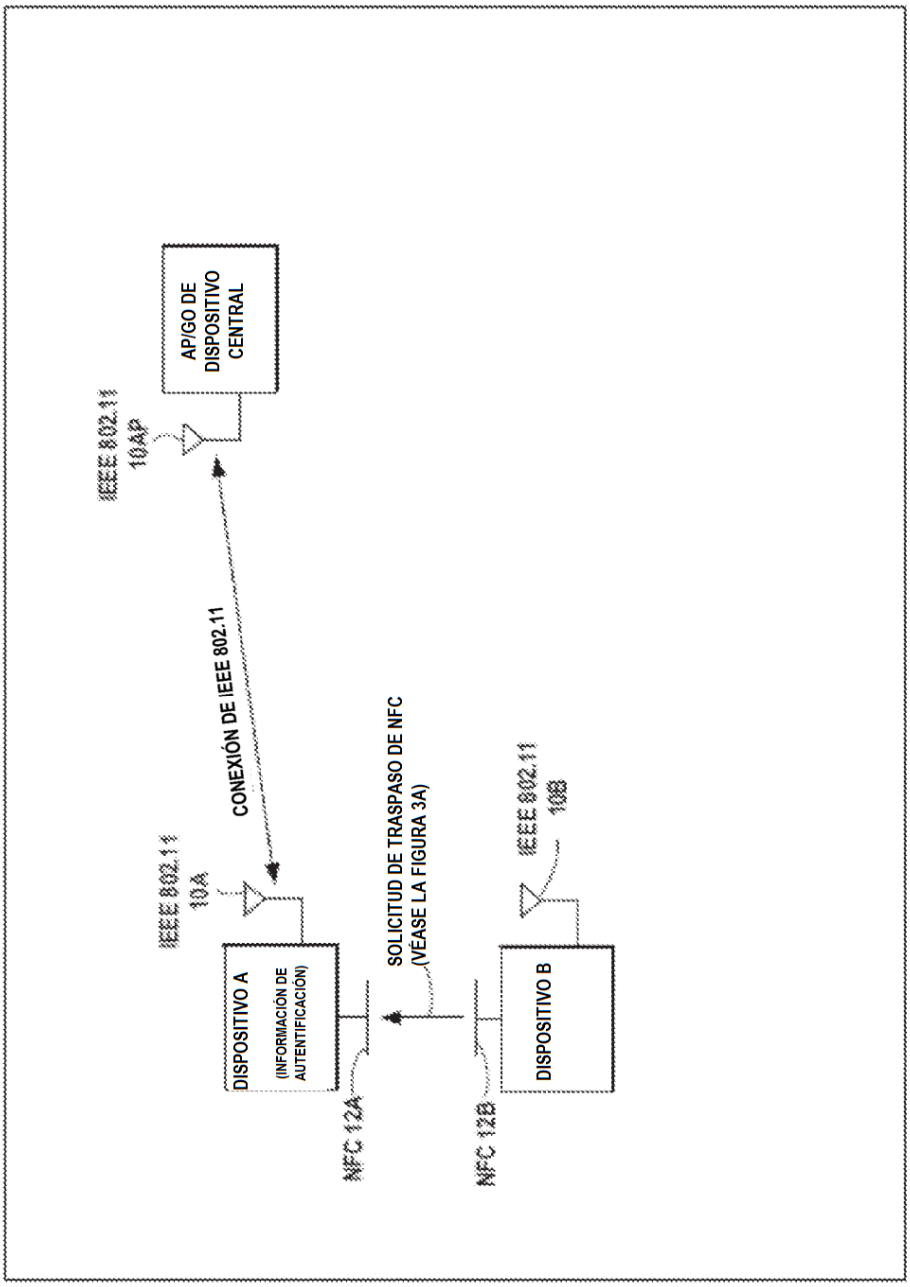

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A
(INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A
SOLICITUD DE TRASPASO DE NFC
(VÉASE LA FIGURA 3A)
NFC 12B
IEEE 802.11 10B
DISPOSITIVO B

FIG. 1E

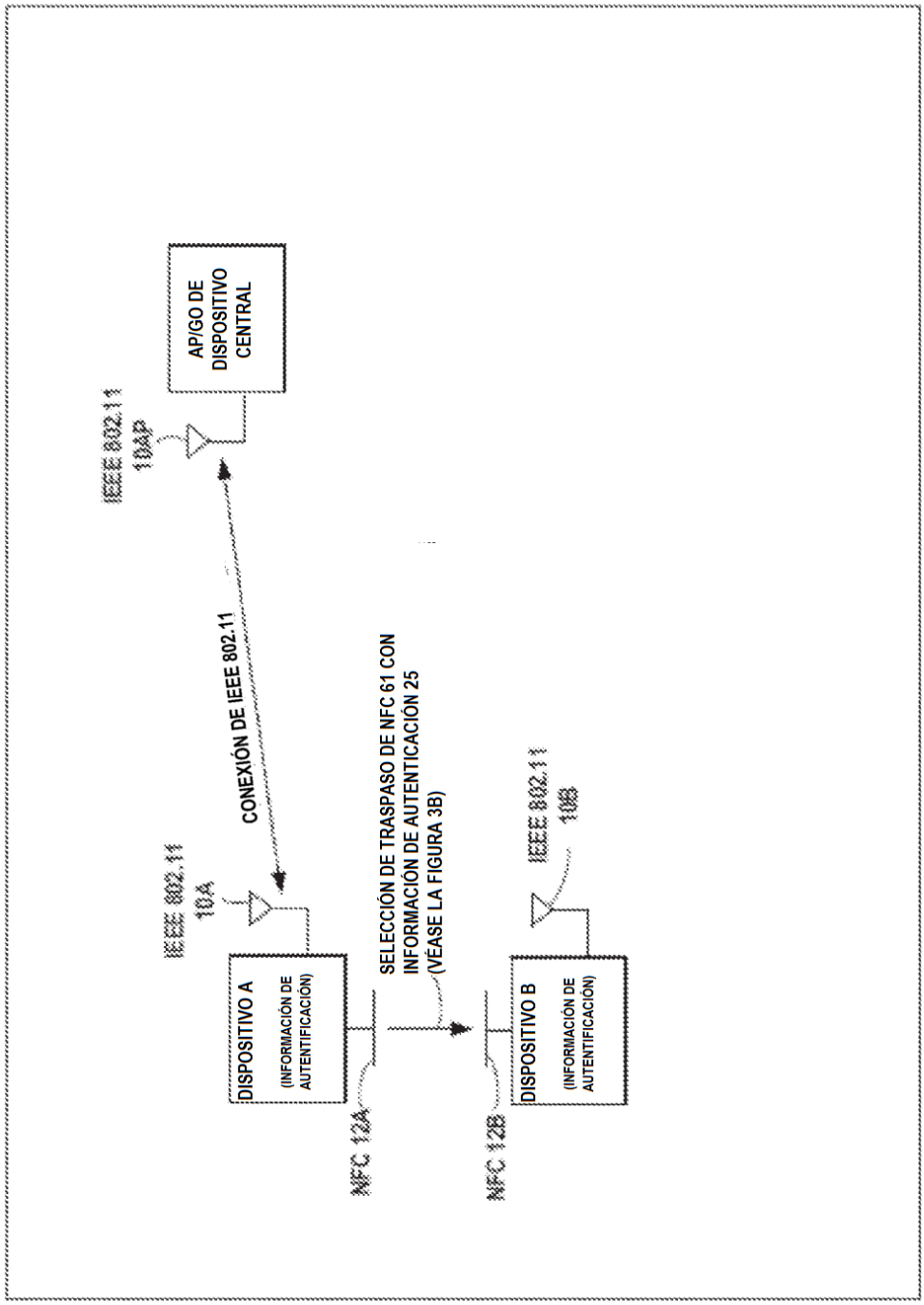

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A
(INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A
SELECCIÓN DE TRASPASO DE NFC 61 CON INFORMACIÓN DE AUTENTICACIÓN 25
(VÉASE LA FIGURA 3B)
NFC 12B
IEEE 802.11 10B
DISPOSITIVO B
(INFORMACIÓN DE AUTENTIFICACIÓN)

FIG. 1F

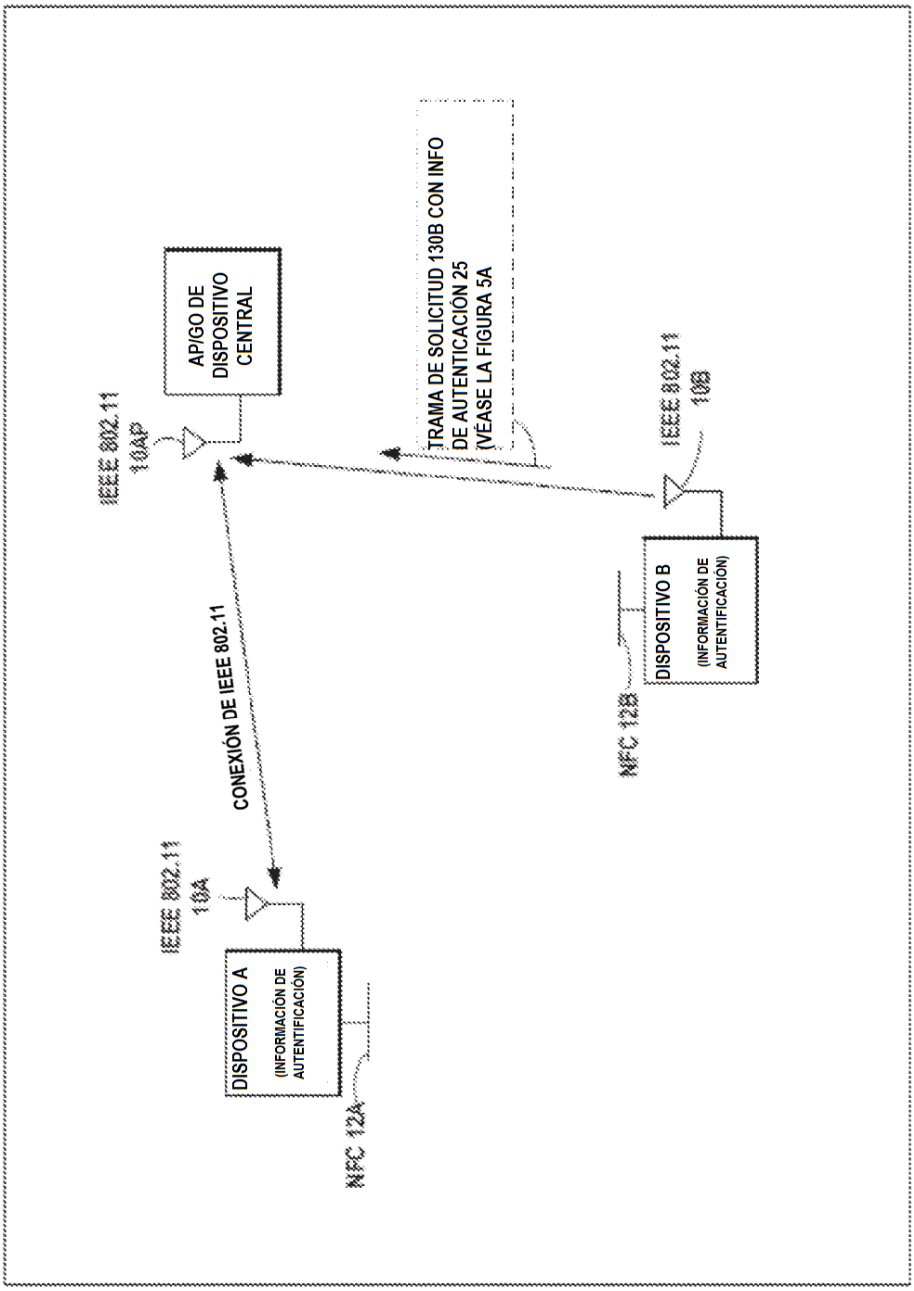

IEEE 802.11
10AP
AP/GO DE
DISPOSITIVO
CENTRAL
TRAMA DE SOLICITUD 130B CON INFO
DE AUTENTICACIÓN 25
(VÉASE LA FIGURA 5A
IEEE 802.11
10B
CONEXIÓN DE IEEE 802.11
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12A
NFC 12B
DISPOSITIVO B
(INFORMACIÓN DE
AUTENTIFICACIÓN)

FIG. 1G

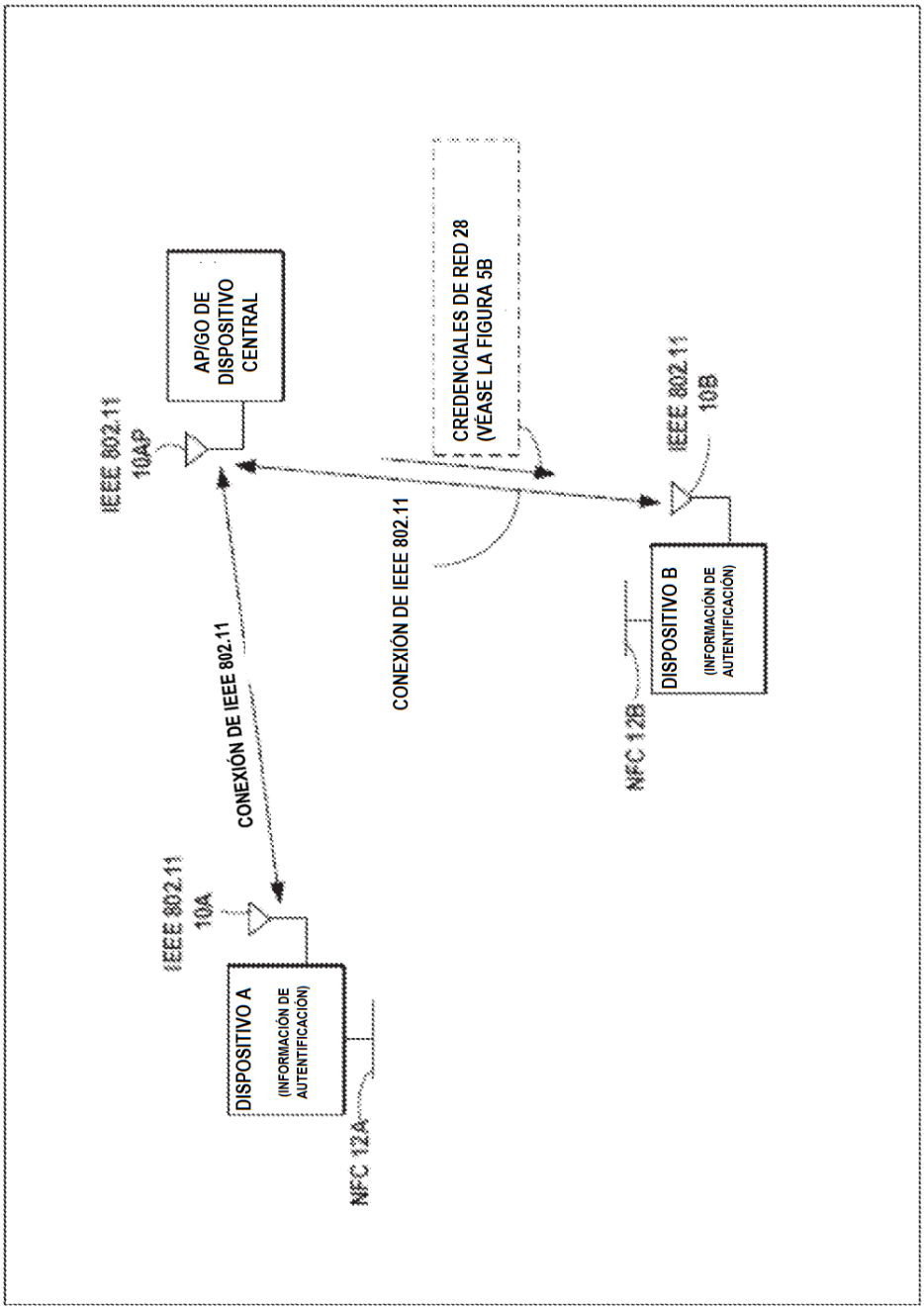

IEEE 802.11
10AP
AP/GO DE
DISPOSITIVO
CENTRAL
CREDENCIALES DE RED 28
(VÉASE LA FIGURA 5B
IEEE 802.11
10B
CONEXIÓN DE IEEE 802.11
CONEXIÓN DE IEEE 802.11
DISPOSITIVO B
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12B
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12A

FIG. 1H

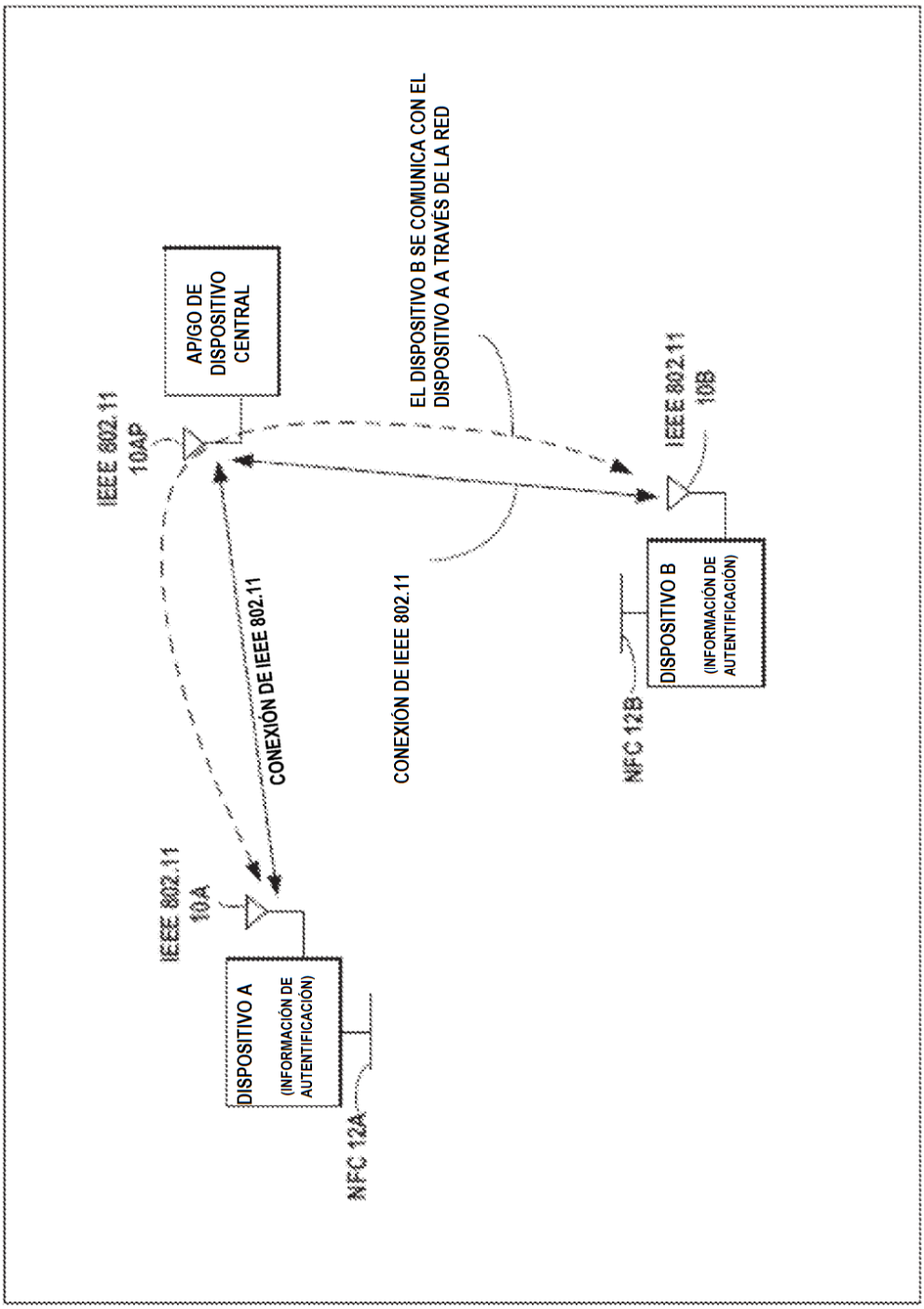

IEEE 802.11
10AP
AP/GO DE
DISPOSITIVO
CENTRAL
EL DISPOSITIVO B SE COMUNICA CON EL
DISPOSITIVO A A TRAVÉS DE LA RED
IEEE 802.11
10B
CONEXIÓN DE IEEE 802.11
CONEXIÓN DE IEEE 802.11
DISPOSITIVO B
(INFORMACIÓN DE
AUTENTIFICACIÓN)
MFC 12B
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE
AUTENTIFICACIÓN)
MFC 12A

FIG. 1I

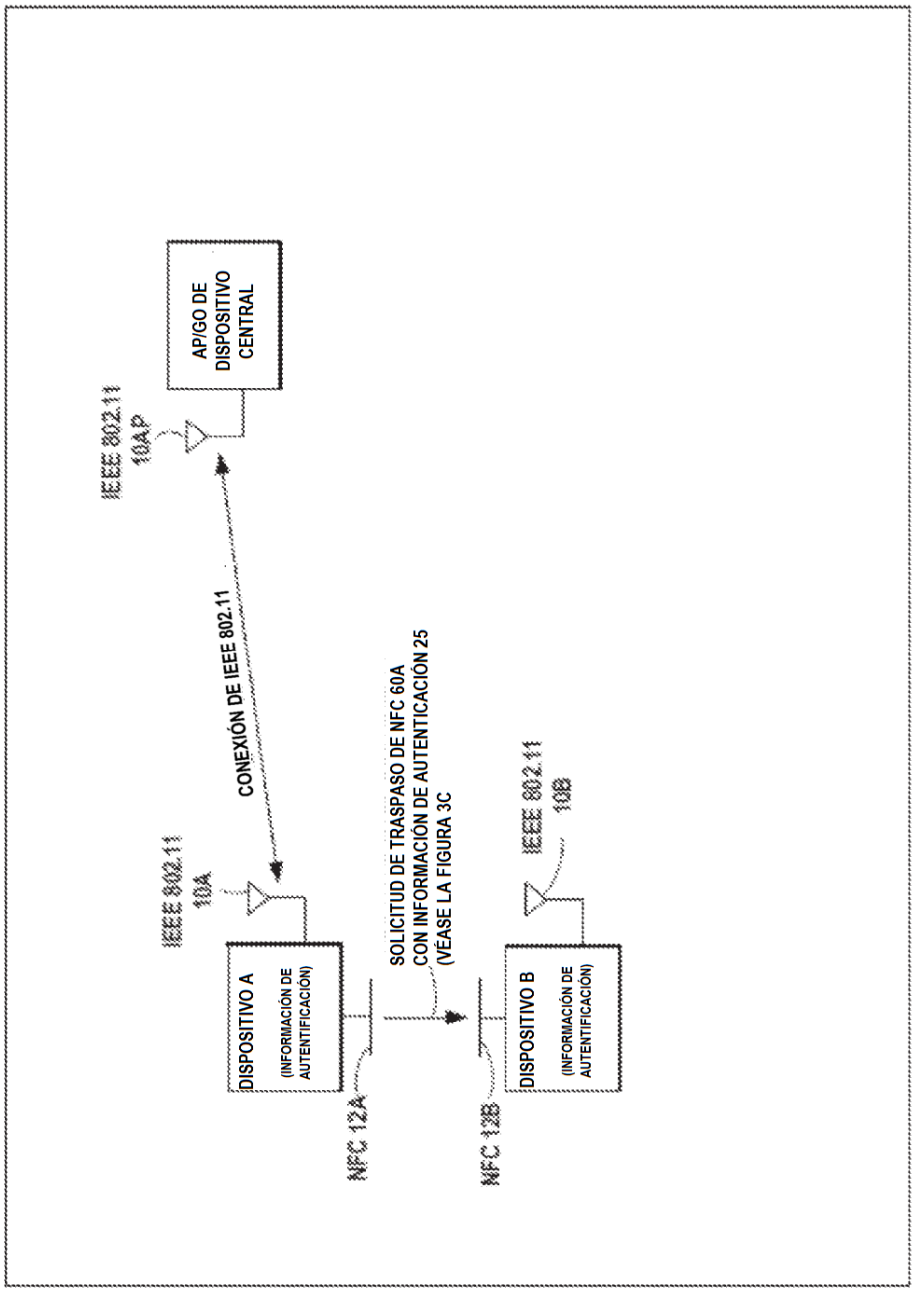

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A (INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A
SOLICITUD DE TRASPASO DE NFC 60A CON INFORMACIÓN DE AUTENTICACIÓN 25 (VÉASE LA FIGURA 3C
NFC 12B
DISPOSITIVO B (INFORMACIÓN DE AUTENTIFICACIÓN)
IEEE 802.11 10B

FIG. 1J

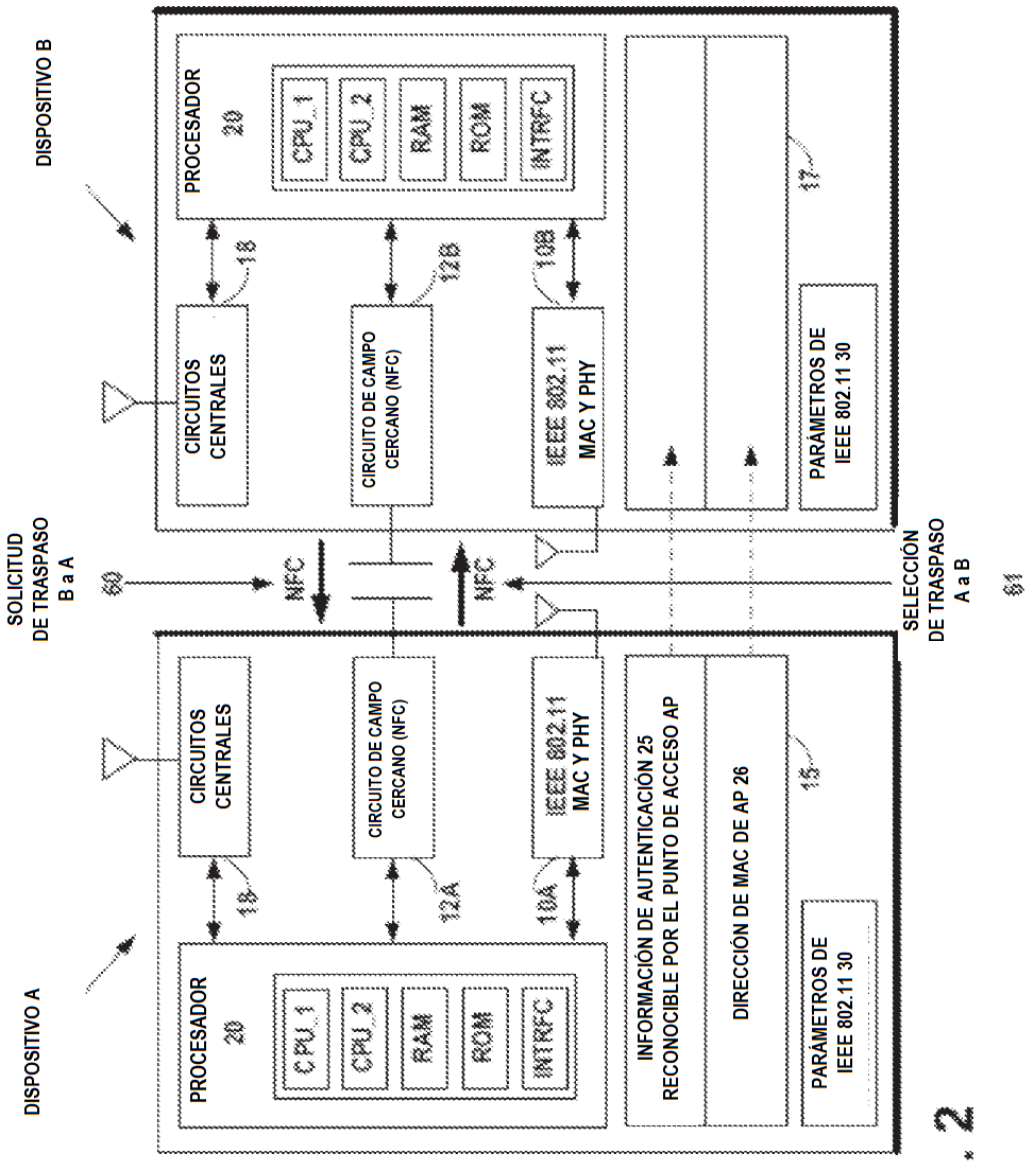

DISPOSITIVO B
PROCESADOR
20
CPU_1
CPU_2
RAM
ROM
INTRFC
CIRCUITOS CENTRALES
18
CIRCUITO DE CAMPO CERCANO (NFC)
12B
IEEE 802.11 MAC Y PHY
10B
PARÁMETROS DE IEEE 802.11 30
17
SOLICITUD DE TRASPASO B a A
60
NFC
NFC
SELECCIÓN DE TRASPASO A a B
61
DISPOSITIVO A
PROCESADOR
20
CPU_1
CPU_2
RAM
ROM
INTRFC
CIRCUITOS CENTRALES
18
CIRCUITO DE CAMPO CERCANO (NFC)
12A
IEEE 802.11 MAC Y PHY
10A
INFORMACIÓN DE AUTENTICACIÓN 25 RECONOCIBLE POR EL PUNTO DE ACCESO AP
DIRECCIÓN DE MAC DE AP 26
15
PARÁMETROS DE IEEE 802.11 30

FIG. 2

FIG. 3A

REGISTRO DE SOLICITUD DE TRASPASO
REGISTRO DE NDEF
REGISTRO DE NDEF
SOLICITUD DE TRASPASO DE NFC B a A
CAMPO DE VERSIÓN
REGISTRO DE PORTADORA ALTERNATIVO
IEEE 802.11
DATOS DE PORTADORA
CONFIGURACIÓN DE PORTADORA
DATOS AUXILIARES
60
(VÉASE LA FIGURA 1E)

FIG. 3B

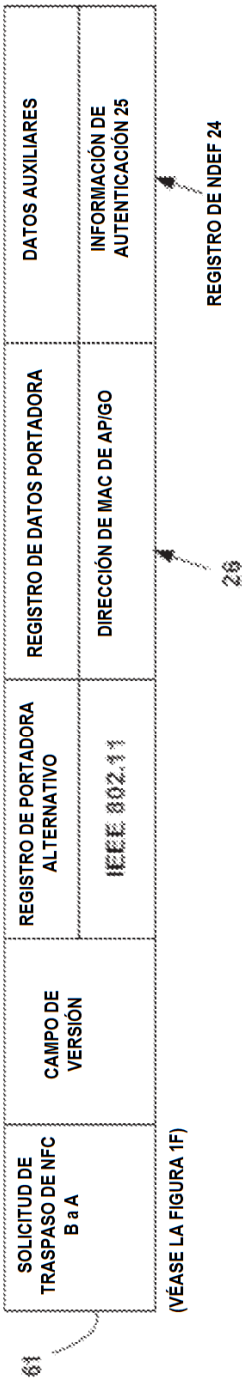
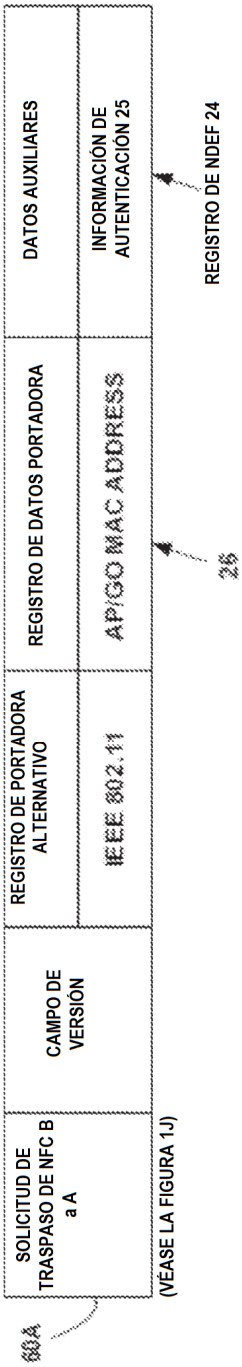

REGISTRO DE SOLICITUD DE TRASPASO
REGISTRO DE NDEF
REGISTRO DE NDEF
SOLICITUD DE TRASPASO DE NFC B a A
CAMPO DE VERSIÓN
REGISTRO DE PORTADORA ALTERNATIVO
IEEE 802.11
REGISTRO DE DATOS PORTADORA
DIRECCIÓN DE MAC DE AP/GO
INFORMACIÓN DE AUTENTICACIÓN 25
DATOS AUXILIARES
61
(VÉASE LA FIGURA 1F)
26
REGISTRO DE NDEF 24

FIG. 3C


REGISTRO DE SOLICITUD DE TRASPASO
REGISTRO DE NDEF
REGISTRO DE NDEF
SOLICITUD DE TRASPASO DE NFC B a A
CAMPO DE VERSIÓN
REGISTRO DE PORTADORA ALTERNATIVO
REGISTRO DE DATOS PORTADORA
DATOS AUXILIARES
IEEE 802.11
APIGO MAC ADDRESS
INFORMACIÓN DE AUTENTICACIÓN 25
(VÉASE LA FIGURA 1J)
REGISTRO DE NDEF 24
26
63A

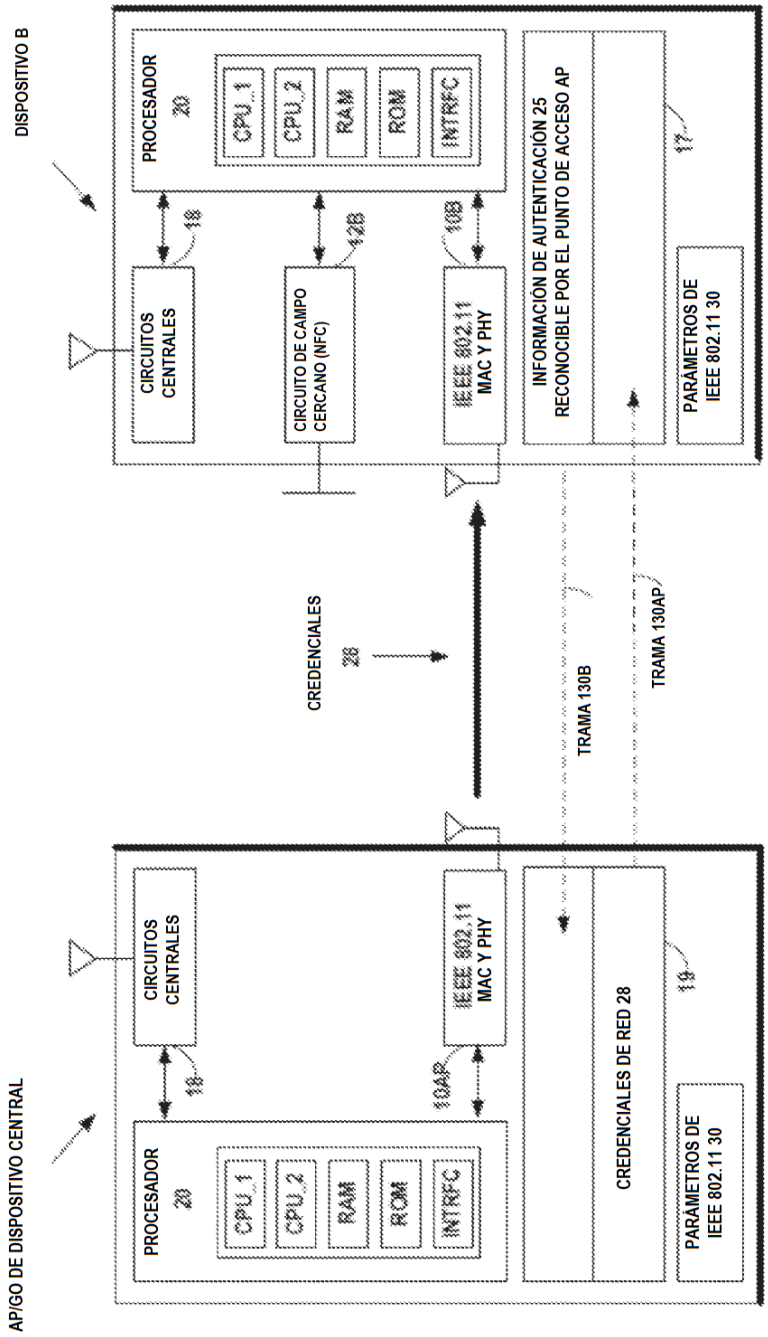

DISPOSITIVO B
PROCESADOR
20
CPU_1
CPU_2
RAM
ROM
INTRFC
18
CIRCUITOS CENTRALES
12B
CIRCUITO DE CAMPO CERCANO (NFC)
10B
IEEE 802.11 MAC Y PHY
INFORMACIÓN DE AUTENTICACIÓN 25 RECONOCIBLE POR EL PUNTO DE ACCESO AP
17
PARÁMETROS DE IEEE 802.11 30
CREDENCIALES
28
TRAMA 130B
TRAMA 130AP
AP/GO DE DISPOSITIVO CENTRAL
PROCESADOR
20
CPU_1
CPU_2
RAM
ROM
INTRFC
18
CIRCUITOS CENTRALES
10AP
IEEE 802.11 MAC Y PHY
CREDENCIALES DE RED 28
19
PARÁMETROS DE IEEE 802.11 30

FIG. 4

FIG. 5A

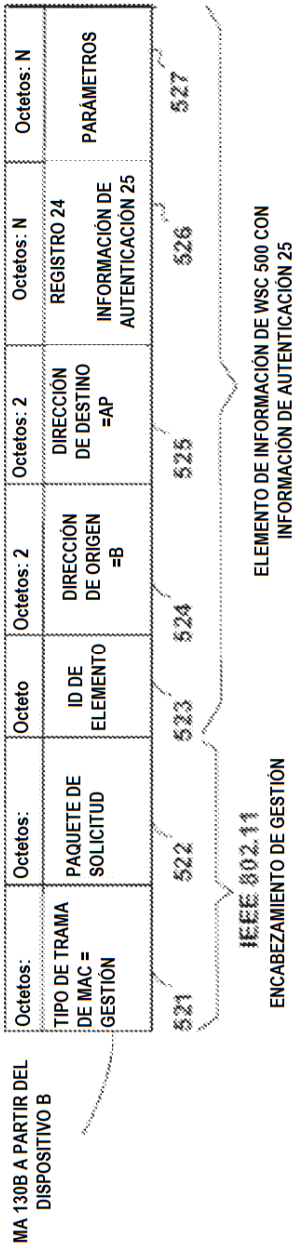

MA 130B A PARTIR DEL DISPOSITIVO B
Octetos:
TIPO DE TRAMA DE MAC = GESTIÓN
Octetos:
PAQUETE DE SOLICITUD
Octeto
ID DE ELEMENTO
Octetos: 2
DIRECCIÓN DE ORIGEN =B
Octetos: 2
DIRECCIÓN DE DESTINO =AP
Octetos: N
REGISTRO 24
INFORMACIÓN DE AUTENTICACIÓN 25
Octetos: N
PARÁMETROS
521
522
523
524
525
526
527
IEEE 802.11
ENCABEZAMIENTO DE GESTIÓN
ELEMENTO DE INFORMACIÓN DE WSC 500 CON INFORMACIÓN DE AUTENTICACIÓN 25

FIG. 5B

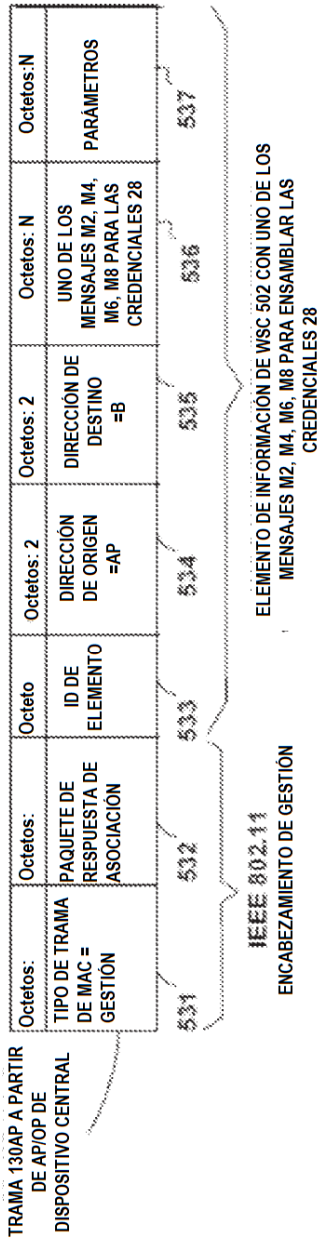
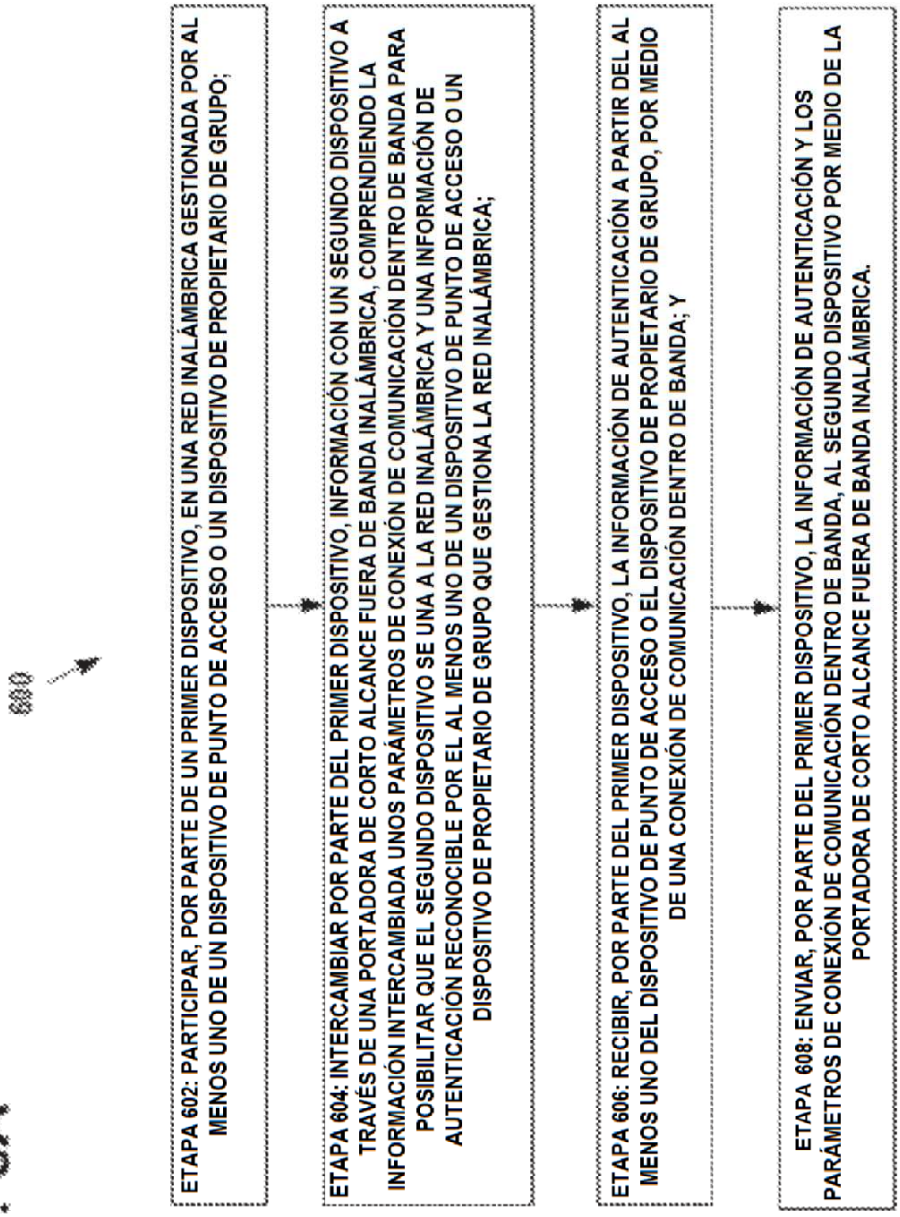

TRAMA 130AP A PARTIR DE AP/OP DE DISPOSITIVO CENTRAL
Octetos:
TIPO DE TRAMA DE MAC = GESTIÓN
Octetos:
PAQUETE DE RESPUESTA DE ASOCIACIÓN
Octeto
ID DE ELEMENTO
Octetos: 2
DIRECCIÓN DE ORIGEN =AP
Octetos: 2
DIRECCIÓN DE DESTINO =B
Octetos: N
UNO DE LOS MENSAJES M2, M4, M6, M8 PARA LAS CREDENCIALES 28
Octetos:N
PARÁMETROS
531
532
533
534
535
536
537
IEEE 802.11
ENCABEZAMIENTO DE GESTIÓN
ELEMENTO DE INFORMACIÓN DE WSC 502 CON UNO DE LOS MENSAJES M2, M4, M6, M8 PARA ENSAMBLAR LAS CREDENCIALES 28

FIG. 6A


600
ETAPA 602: PARTICIPAR, POR PARTE DE UN PRIMER DISPOSITIVO, EN UNA RED INALÁMBRICA GESTIONADA POR AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO;
ETAPA 604: INTERCAMBIAR POR PARTE DEL PRIMER DISPOSITIVO, INFORMACIÓN CON UN SEGUNDO DISPOSITIVO A TRAVÉS DE UNA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, COMPRENDIENDO LA INFORMACIÓN INTERCAMBIADA UNOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA PARA POSIBILITAR QUE EL SEGUNDO DISPOSITIVO SE UNA A LA RED INALÁMBRICA Y UNA INFORMACIÓN DE AUTENTICACIÓN RECONOCIBLE POR EL AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO QUE GESTIONA LA RED INALÁMBRICA;
ETAPA 606: RECIBIR, POR PARTE DEL PRIMER DISPOSITIVO, LA INFORMACIÓN DE AUTENTICACIÓN A PARTIR DEL AL MENOS UNO DEL DISPOSITIVO DE PUNTO DE ACCESO O EL DISPOSITIVO DE PROPIETARIO DE GRUPO, POR MEDIO DE UNA CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA; Y
ETAPA 608: ENVIAR, POR PARTE DEL PRIMER DISPOSITIVO, LA INFORMACIÓN DE AUTENTICACIÓN Y LOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA, AL SEGUNDO DISPOSITIVO POR MEDIO DE LA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA.

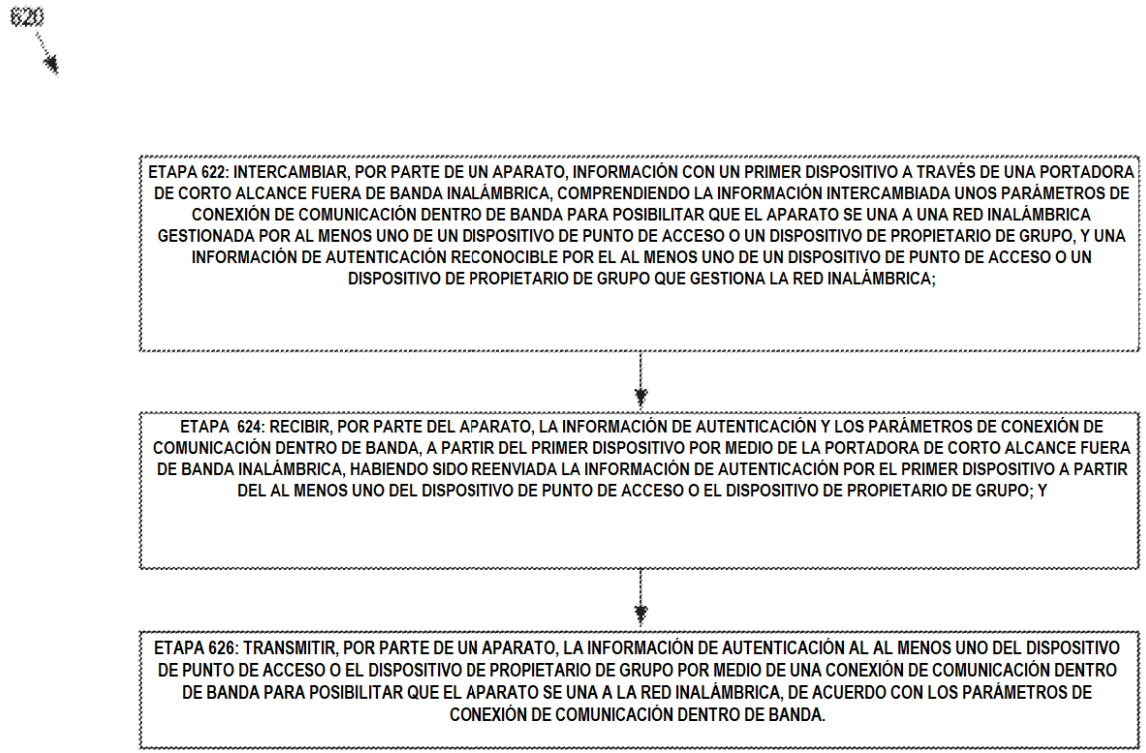

620
ETAPA 622: INTERCAMBIAR, POR PARTE DE UN APARATO, INFORMACIÓN CON UN PRIMER DISPOSITIVO A TRAVÉS DE UNA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, COMPRENDIENDO LA INFORMACIÓN INTERCAMBIADA UNOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA PARA POSIBILITAR QUE EL APARATO SE UNA A UNA RED INALÁMBRICA GESTIONADA POR AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO, Y UNA INFORMACIÓN DE AUTENTICACIÓN RECONOCIBLE POR EL AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO QUE GESTIONA LA RED INALÁMBRICA;
ETAPA 624: RECIBIR, POR PARTE DEL APARATO, LA INFORMACIÓN DE AUTENTICACIÓN Y LOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA, A PARTIR DEL PRIMER DISPOSITIVO POR MEDIO DE LA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, HABIENDO SIDO REENVIADA LA INFORMACIÓN DE AUTENTICACIÓN POR EL PRIMER DISPOSITIVO A PARTIR DEL AL MENOS UNO DEL DISPOSITIVO DE PUNTO DE ACCESO O EL DISPOSITIVO DE PROPIETARIO DE GRUPO; Y
ETAPA 626: TRANSMITIR, POR PARTE DE UN APARATO, LA INFORMACIÓN DE AUTENTICACIÓN AL AL MENOS UNO DEL DISPOSITIVO DE PUNTO DE ACCESO O EL DISPOSITIVO DE PROPIETARIO DE GRUPO POR MEDIO DE UNA CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA PARA POSIBILITAR QUE EL APARATO SE UNA A LA RED INALÁMBRICA, DE ACUERDO CON LOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA.

FIG. 6B

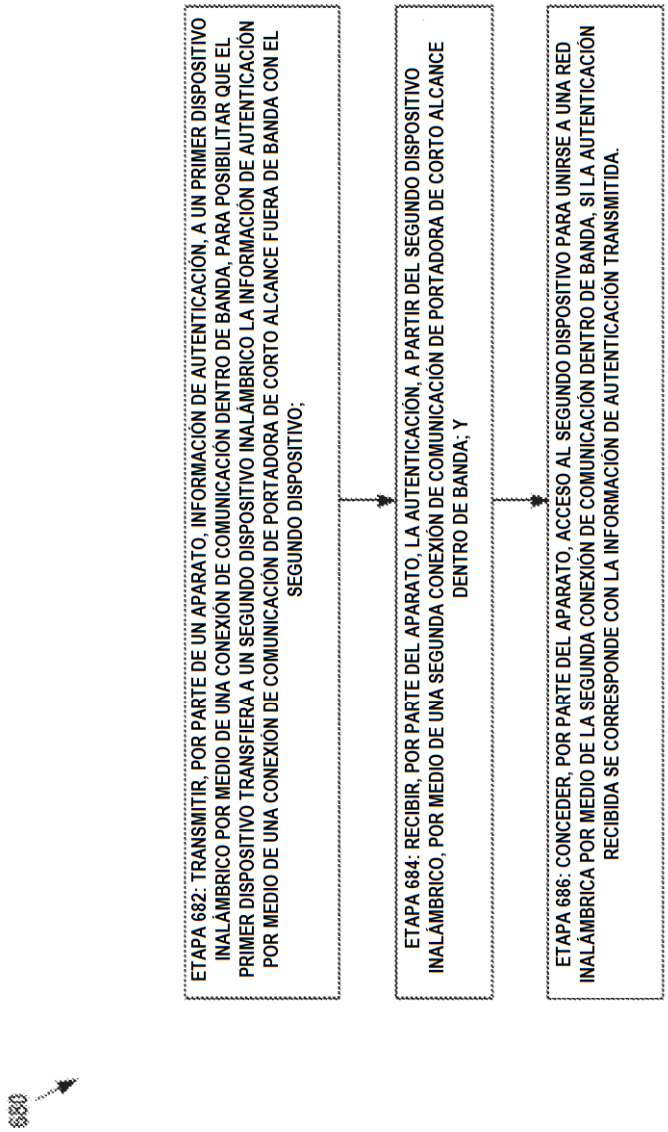

680
ETAPA 682: TRANSMITIR, POR PARTE DE UN APARATO, INFORMACIÓN DE AUTENTICACIÓN, A UN PRIMER DISPOSITIVO INALÁMBRICO POR MEDIO DE UNA CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA, PARA POSIBILITAR QUE EL PRIMER DISPOSITIVO TRANSFIERA A UN SEGUNDO DISPOSITIVO INALÁMBRICO LA INFORMACIÓN DE AUTENTICACIÓN POR MEDIO DE UNA CONEXIÓN DE COMUNICACIÓN DE PORTADORA DE CORTO ALCANCE FUERA DE BANDA CON EL SEGUNDO DISPOSITIVO;
ETAPA 684: RECIBIR, POR PARTE DEL APARATO, LA AUTENTICACIÓN, A PARTIR DEL SEGUNDO DISPOSITIVO INALÁMBRICO, POR MEDIO DE UNA SEGUNDA CONEXIÓN DE COMUNICACIÓN DE PORTADORA DE CORTO ALCANCE DENTRO DE BANDA; Y
ETAPA 686: CONCEDER, POR PARTE DEL APARATO, ACCESO AL SEGUNDO DISPOSITIVO PARA UNIRSE A UNA RED INALÁMBRICA POR MEDIO DE LA SEGUNDA CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA, SI LA AUTENTICACIÓN RECIBIDA SE CORRESPONDE CON LA INFORMACIÓN DE AUTENTICACIÓN TRANSMITIDA.

FIG. 6C

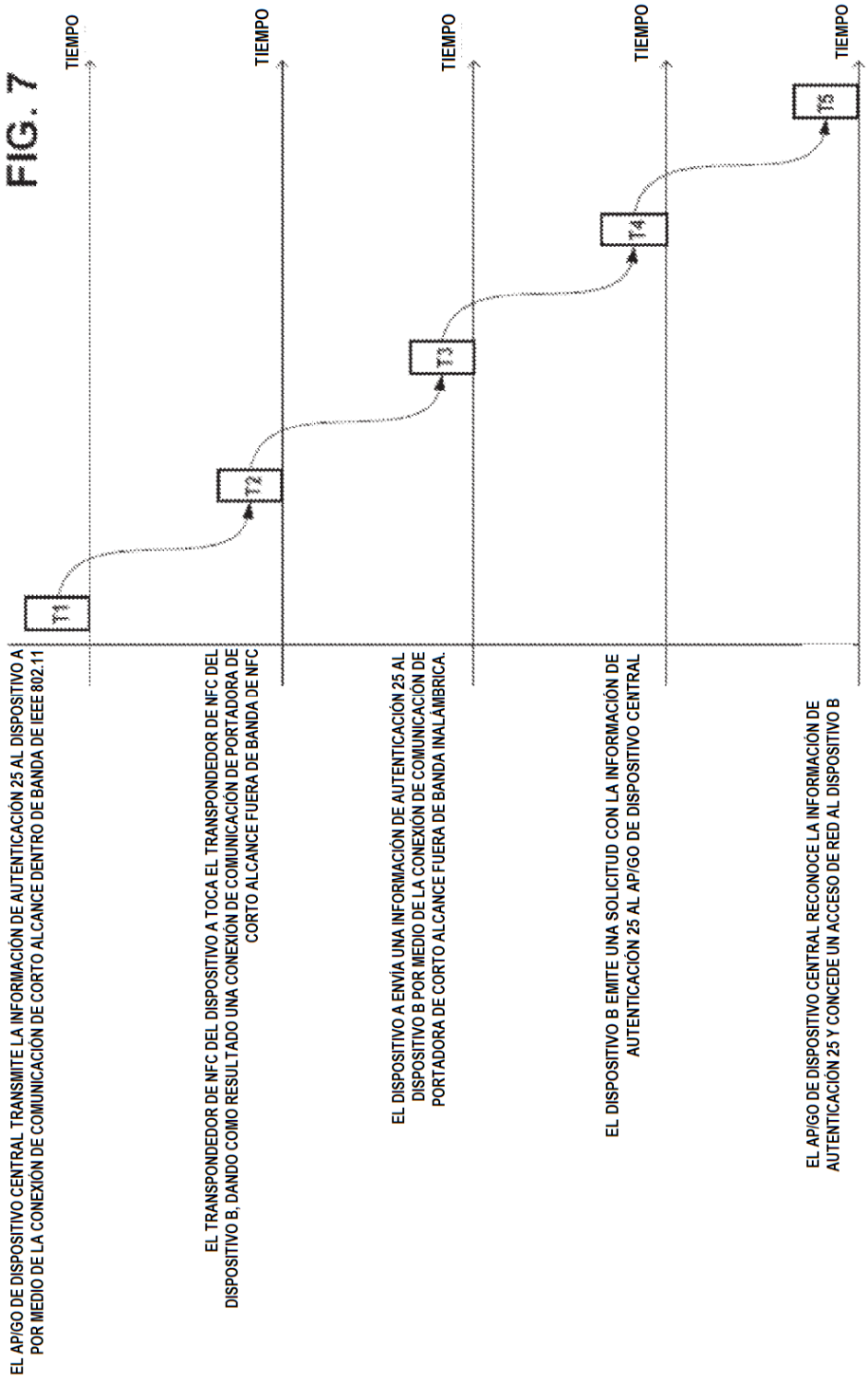


FIG. 7
TIEMPO
TIEMPO
TIEMPO
TIEMPO
TIEMPO
T1
T2
T3
T4
T5
EL AP/GO DE DISPOSITIVO CENTRAL TRANSMITE LA INFORMACIÓN DE AUTENTICACIÓN 25 AL DISPOSITIVO A POR MEDIO DE LA CONEXIÓN DE COMUNICACIÓN DE CORTO ALCANCE DENTRO DE BANDA DE IEEE 802.11
EL TRANSPONDEDOR DE NFC DEL DISPOSITIVO A TOCA EL TRANSPONDEDOR DE NFC DEL DISPOSITIVO B, DANDO COMO RESULTADO UNA CONEXIÓN DE COMUNICACIÓN DE PORTADORA DE CORTO ALCANCE FUERA DE BANDA DE NFC
EL DISPOSITIVO A ENVÍA UNA INFORMACIÓN DE AUTENTICACIÓN 25 AL DISPOSITIVO B POR MEDIO DE LA CONEXIÓN DE COMUNICACIÓN DE PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA.
EL DISPOSITIVO B EMITE UNA SOLICITUD CON LA INFORMACIÓN DE AUTENTICACIÓN 25 AL AP/GO DE DISPOSITIVO CENTRAL
EL AP/GO DE DISPOSITIVO CENTRAL RECONOCE LA INFORMACIÓN DE AUTENTICACIÓN 25 Y CONCEDE UN ACCESO DE RED AL DISPOSITIVO B

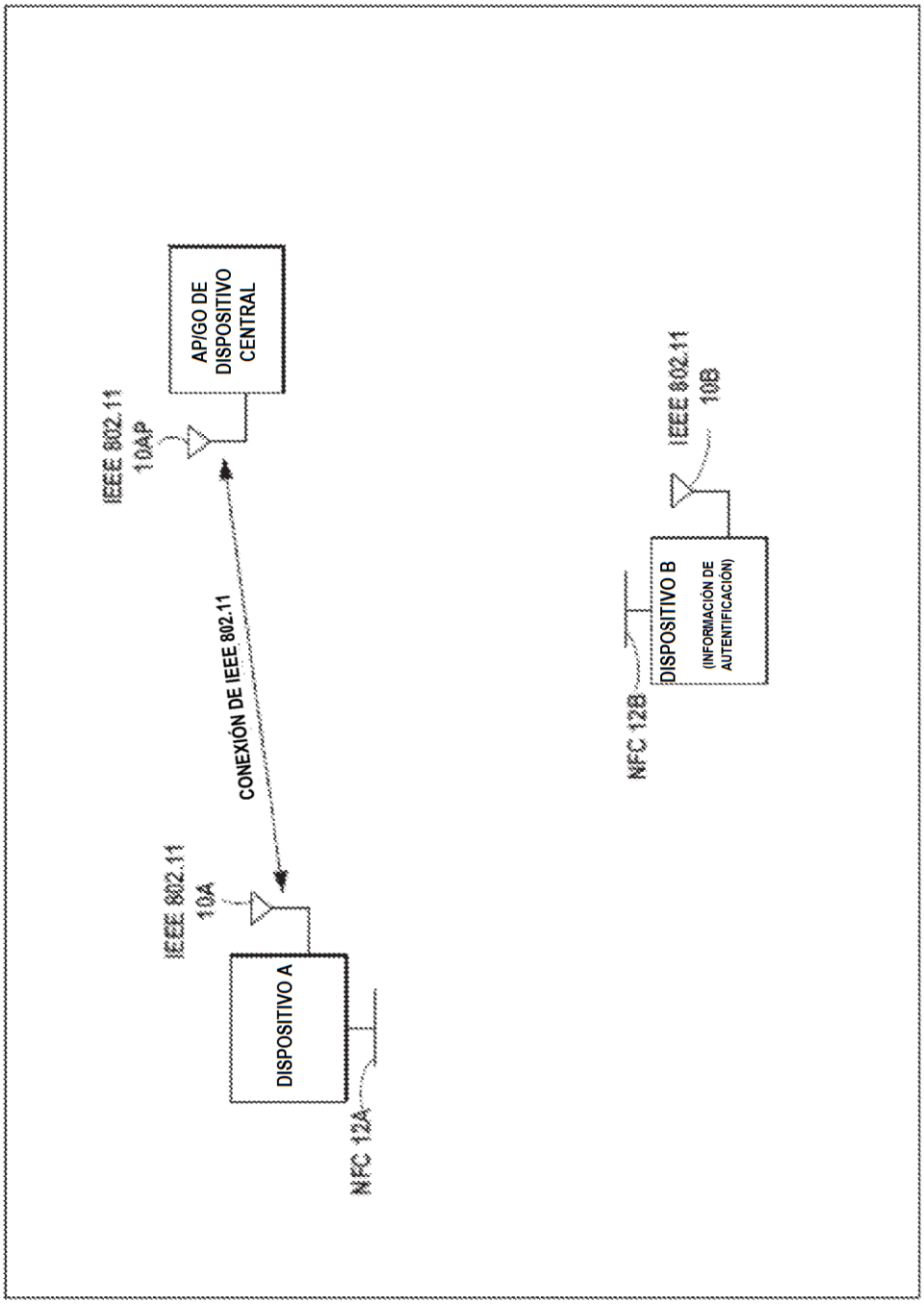

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A
NFC 12A
IEEE 802.11 10B
DISPOSITIVO B
(INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12B

FIG. 8A

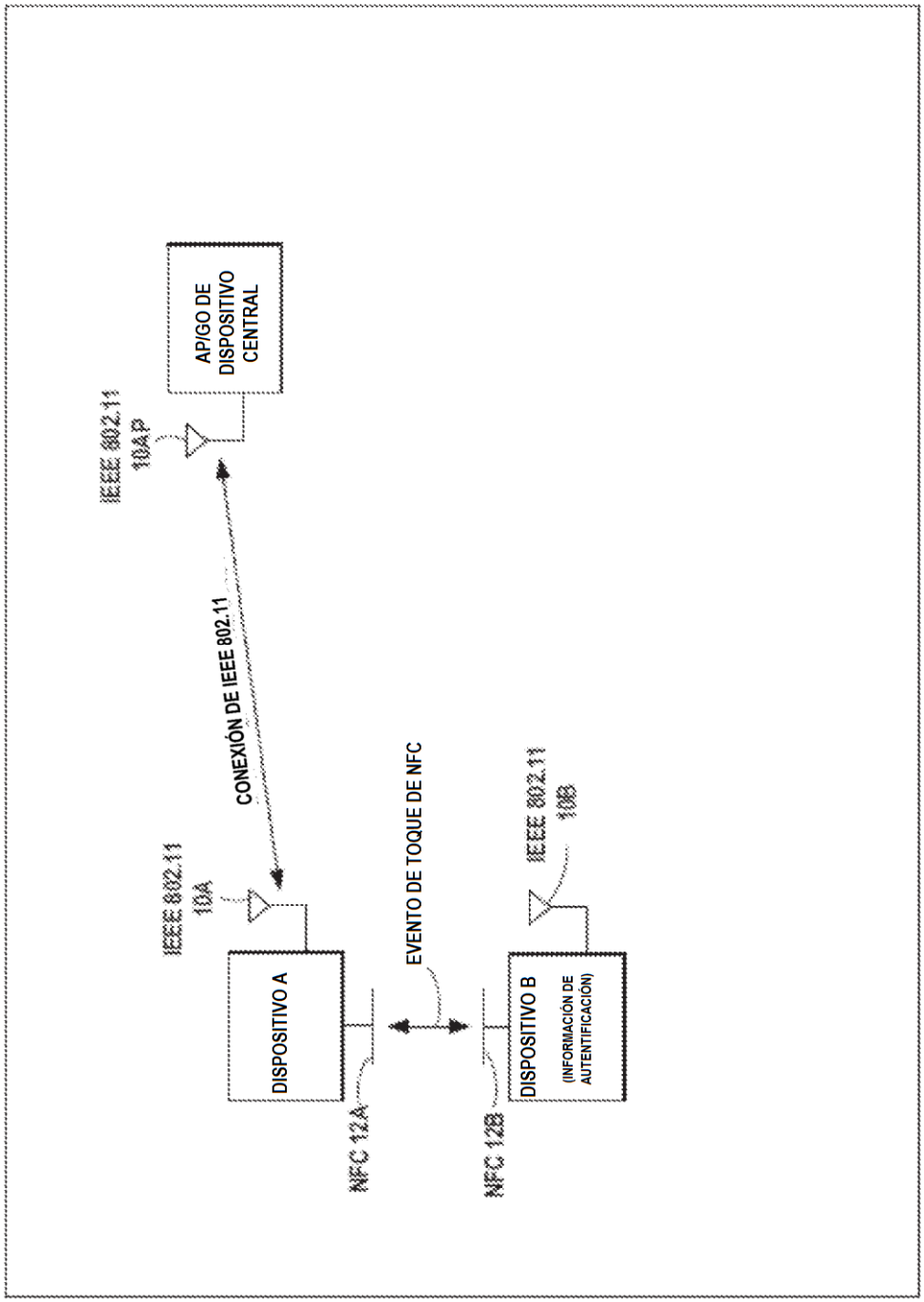

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A
NFC 12A
EVENTO DE TOQUE DE NFC
NFC 12B
DISPOSITIVO B
(INFORMACIÓN DE AUTENTIFICACIÓN)
IEEE 802.11 10B

FIG. 8B

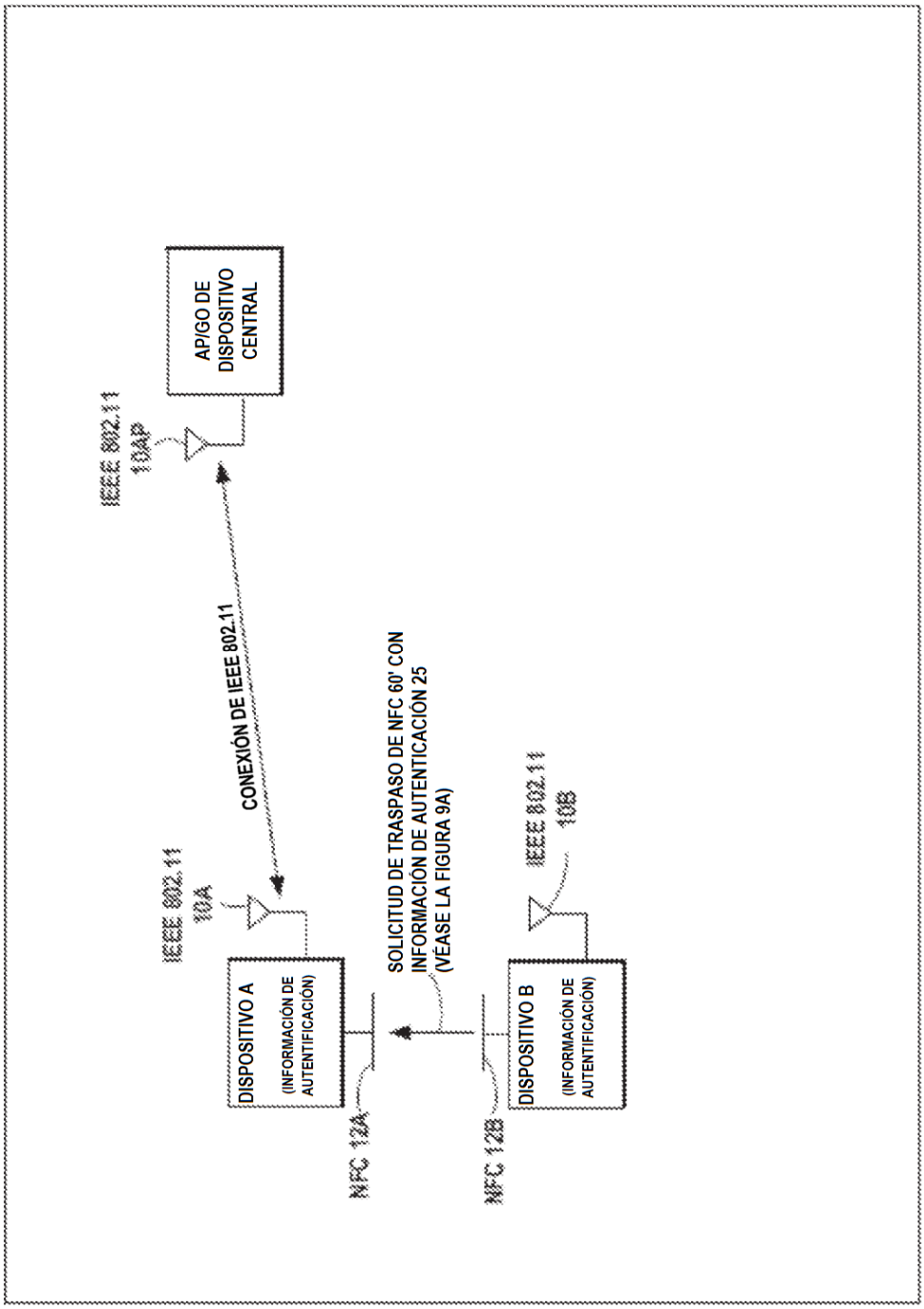

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A (INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A
SOLICITUD DE TRASPASO DE NFC 60' CON INFORMACIÓN DE AUTENTICACIÓN 25 (VÉASE LA FIGURA 9A)
NFC 12B
IEEE 802.11 10B
DISPOSITIVO B (INFORMACIÓN DE AUTENTIFICACIÓN)

FIG. 8C

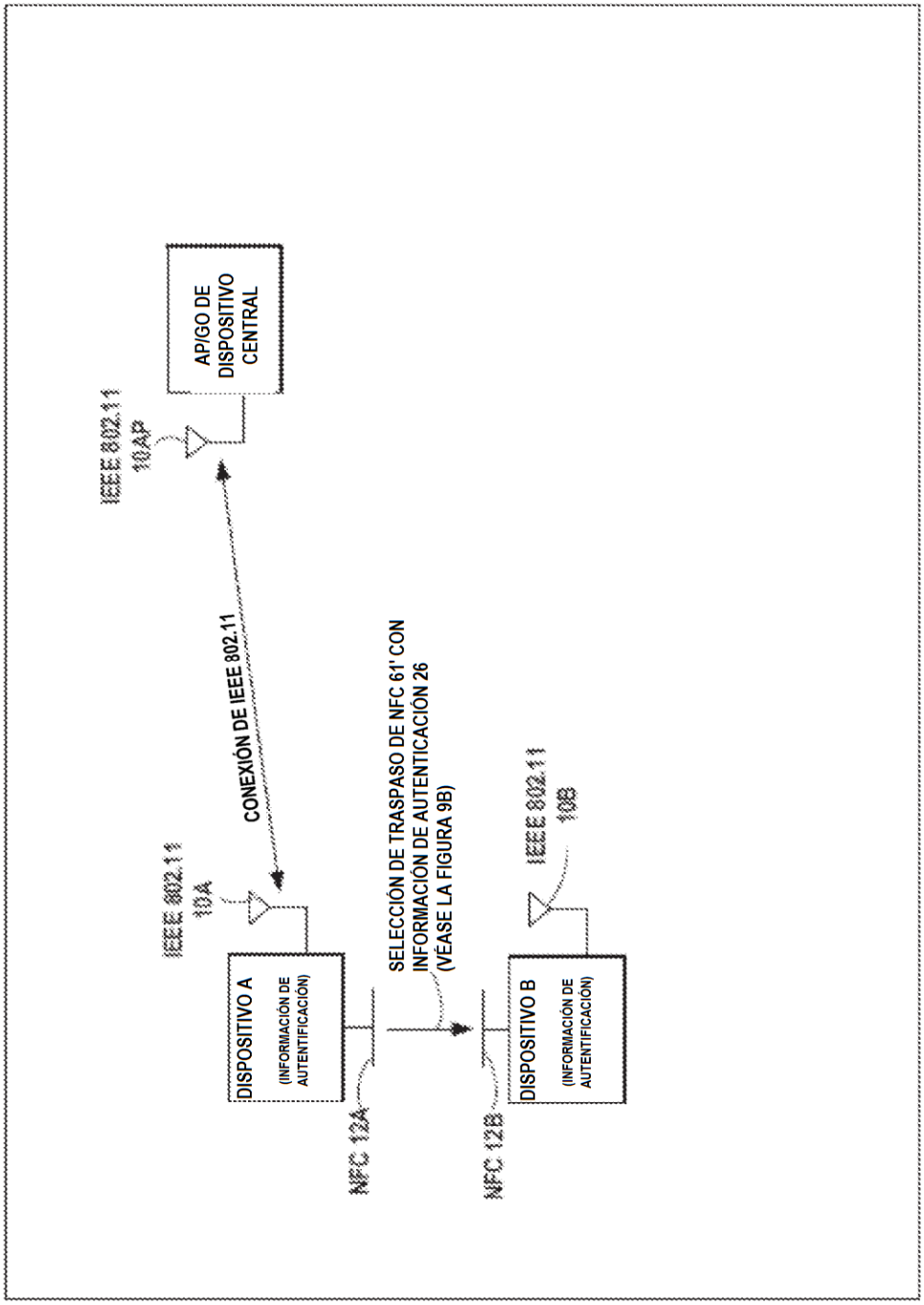

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A
(INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A
SELECCIÓN DE TRASPASO DE NFC 61' CON INFORMACIÓN DE AUTENTICACIÓN 26 (VÉASE LA FIGURA 9B)
NFC 12B
IEEE 802.11 10B
DISPOSITIVO B
(INFORMACIÓN DE AUTENTIFICACIÓN)

FIG. 8D

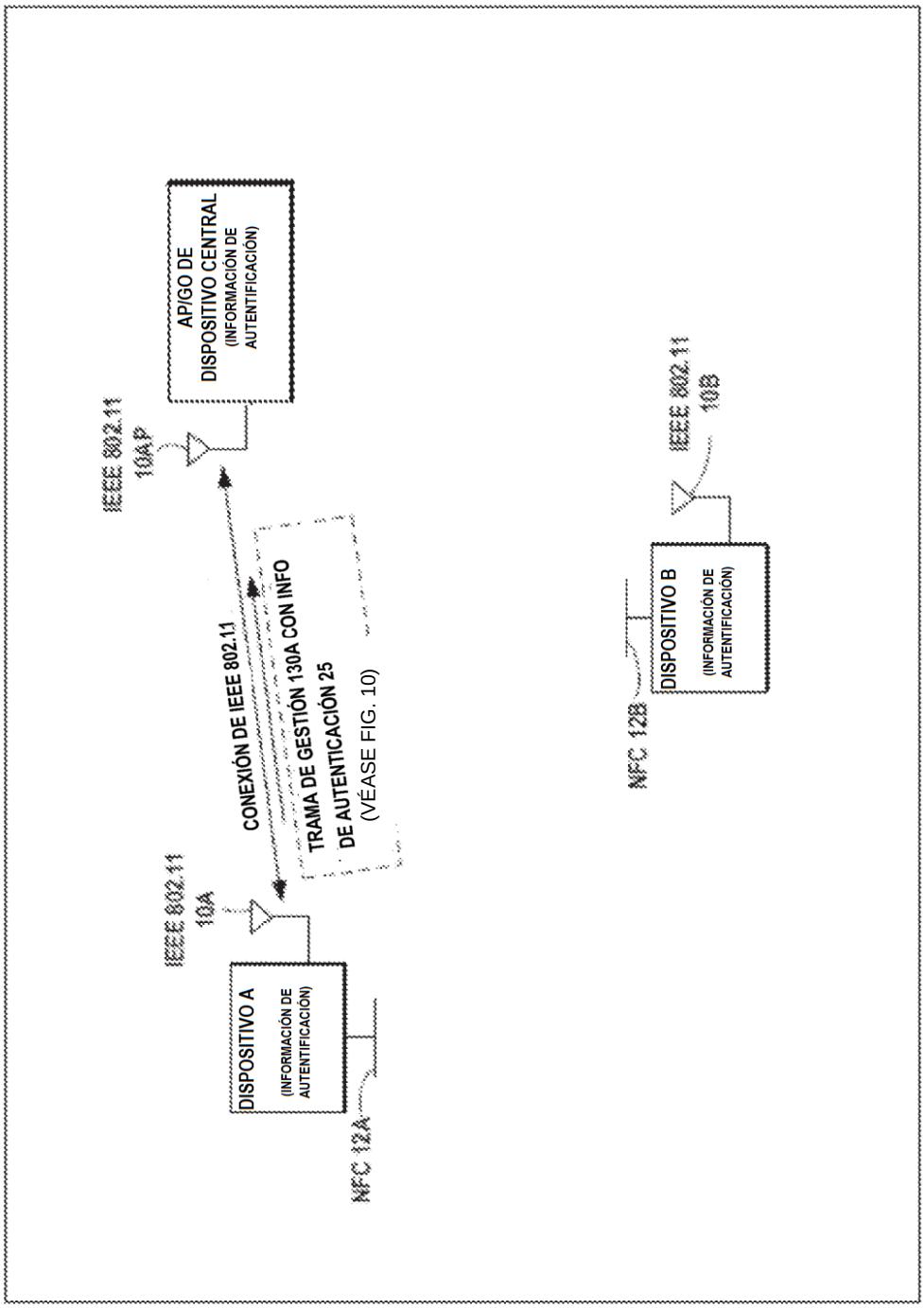

AP/GO DE
DISPOSITIVO CENTRAL
(INFORMACIÓN DE
AUTENTIFICACIÓN)
IEEE 802.11
10AP
CONEXIÓN DE IEEE 802.11
TRAMA DE GESTIÓN 130A CON INFO
DE AUTENTICACIÓN 25
(VÉASE FIG. 10)
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12A
IEEE 802.11
10B
DISPOSITIVO B
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12B

FIG. 8E

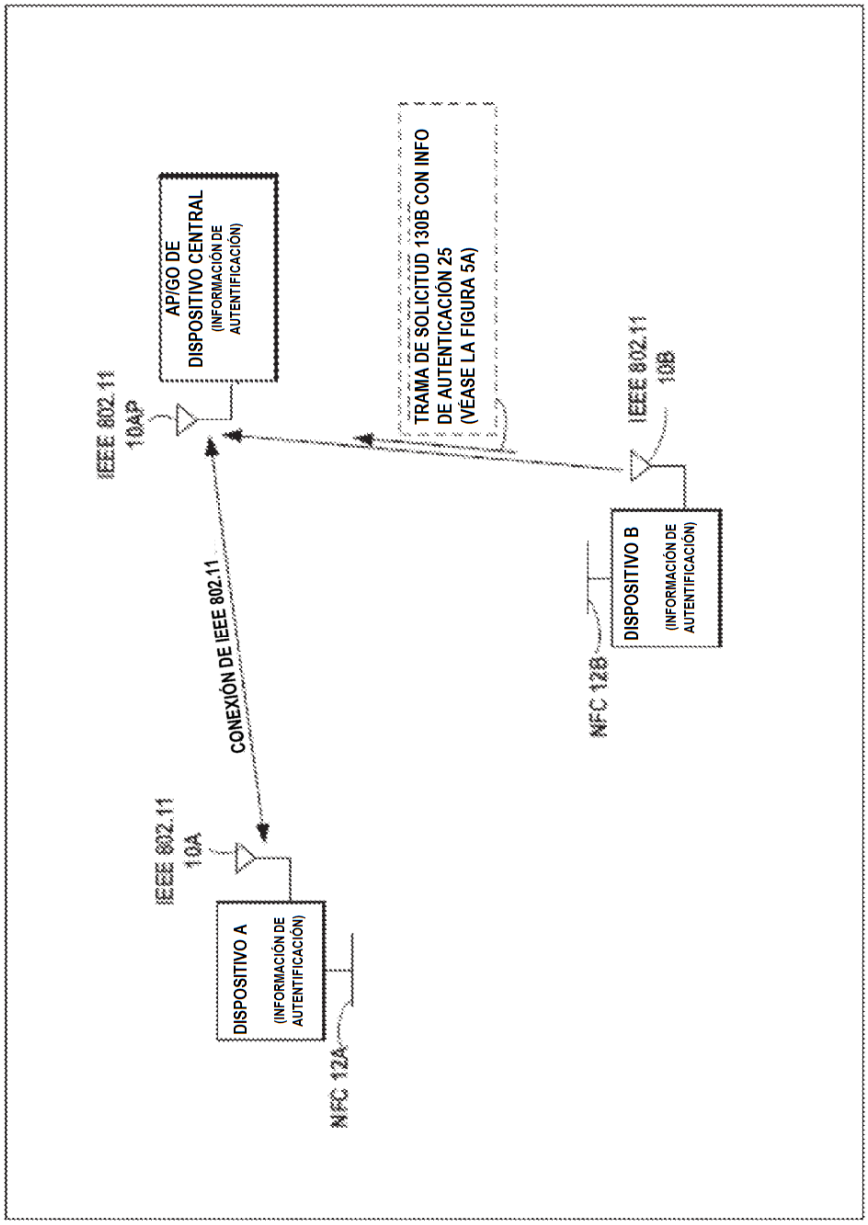

IEEE 802.11
10AP
AP/GO DE
DISPOSITIVO CENTRAL
(INFORMACIÓN DE
AUTENTIFICACIÓN)
CONEXIÓN DE IEEE 802.11
TRAMA DE SOLICITUD 130B CON INFO
DE AUTENTICACIÓN 25
(VÉASE LA FIGURA 5A)
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12A
IEEE 802.11
10B
DISPOSITIVO B
(INFORMACIÓN DE
AUTENTIFICACIÓN)
NFC 12B

FIG. 8F

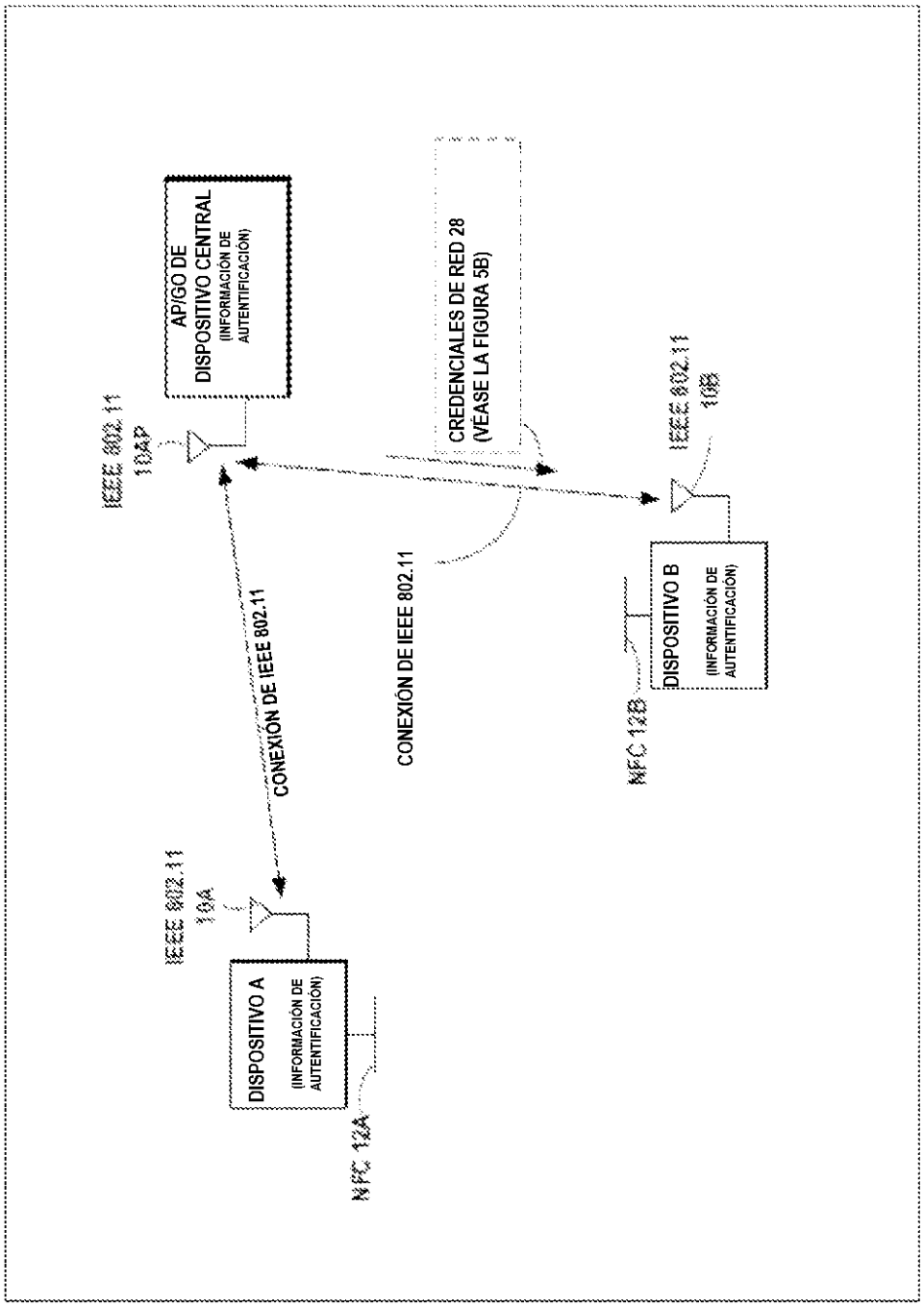

AP/GO DE DISPOSITIVO CENTRAL
(INFORMACIÓN DE AUTENTIFICACIÓN)
IEEE 802.11
10AP
CREDENCIALES DE RED 28
(VÉASE LA FIGURA 5B)
IEEE 802.11
10B
CONEXIÓN DE IEEE 802.11
CONEXIÓN DE IEEE 802.11
DISPOSITIVO B
(INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12B
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A

FIG. 8G

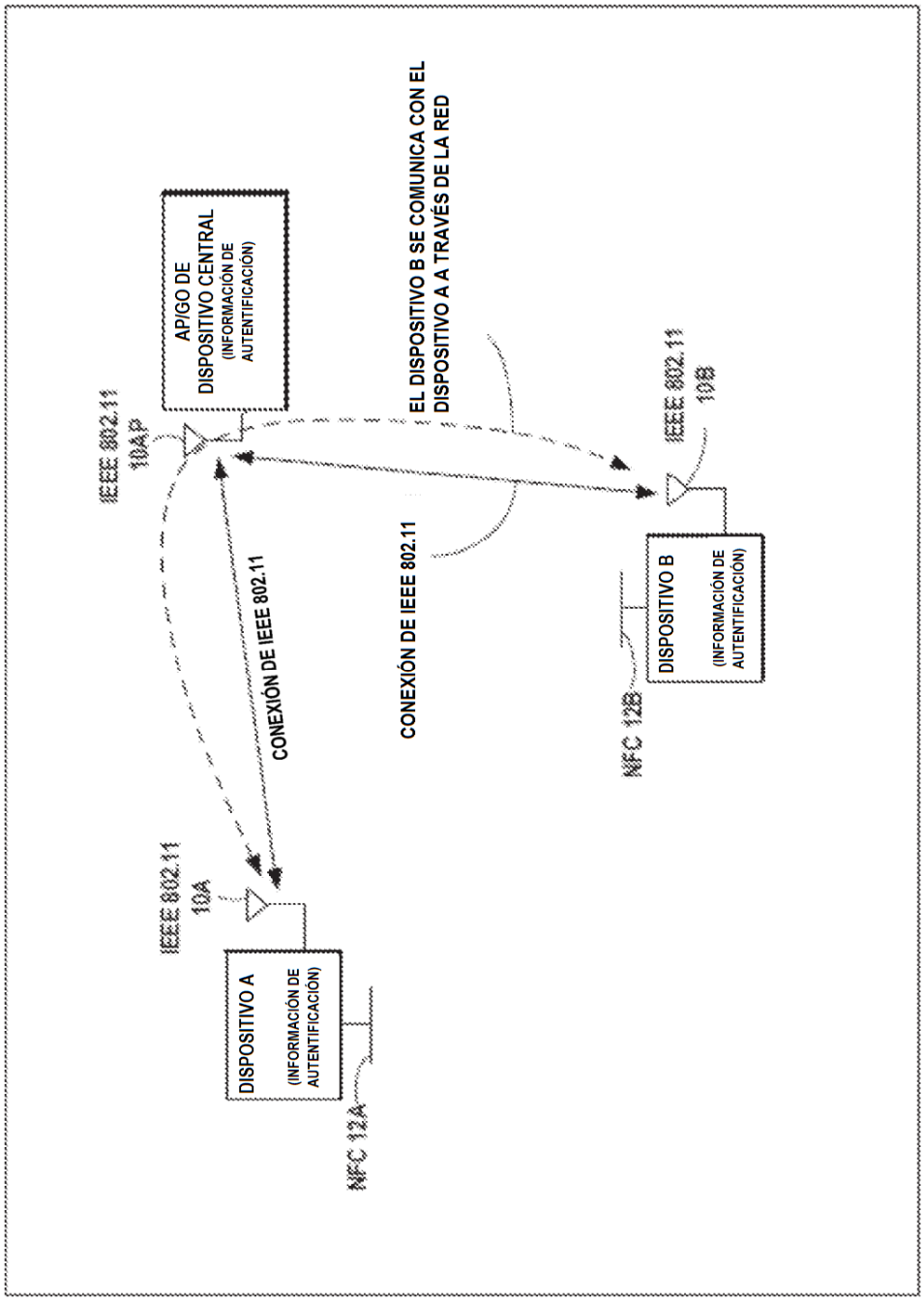

AP/GO DE DISPOSITIVO CENTRAL (INFORMACIÓN DE AUTENTIFICACIÓN)
IEEE 802.11 10AP
EL DISPOSITIVO B SE COMUNICA CON EL DISPOSITIVO A A TRAVÉS DE LA RED
IEEE 802.11 10B
CONEXIÓN DE IEEE 802.11
CONEXIÓN DE IEEE 802.11
DISPOSITIVO B (INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12B
IEEE 802.11 10A
DISPOSITIVO A (INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A

FIG. 8H

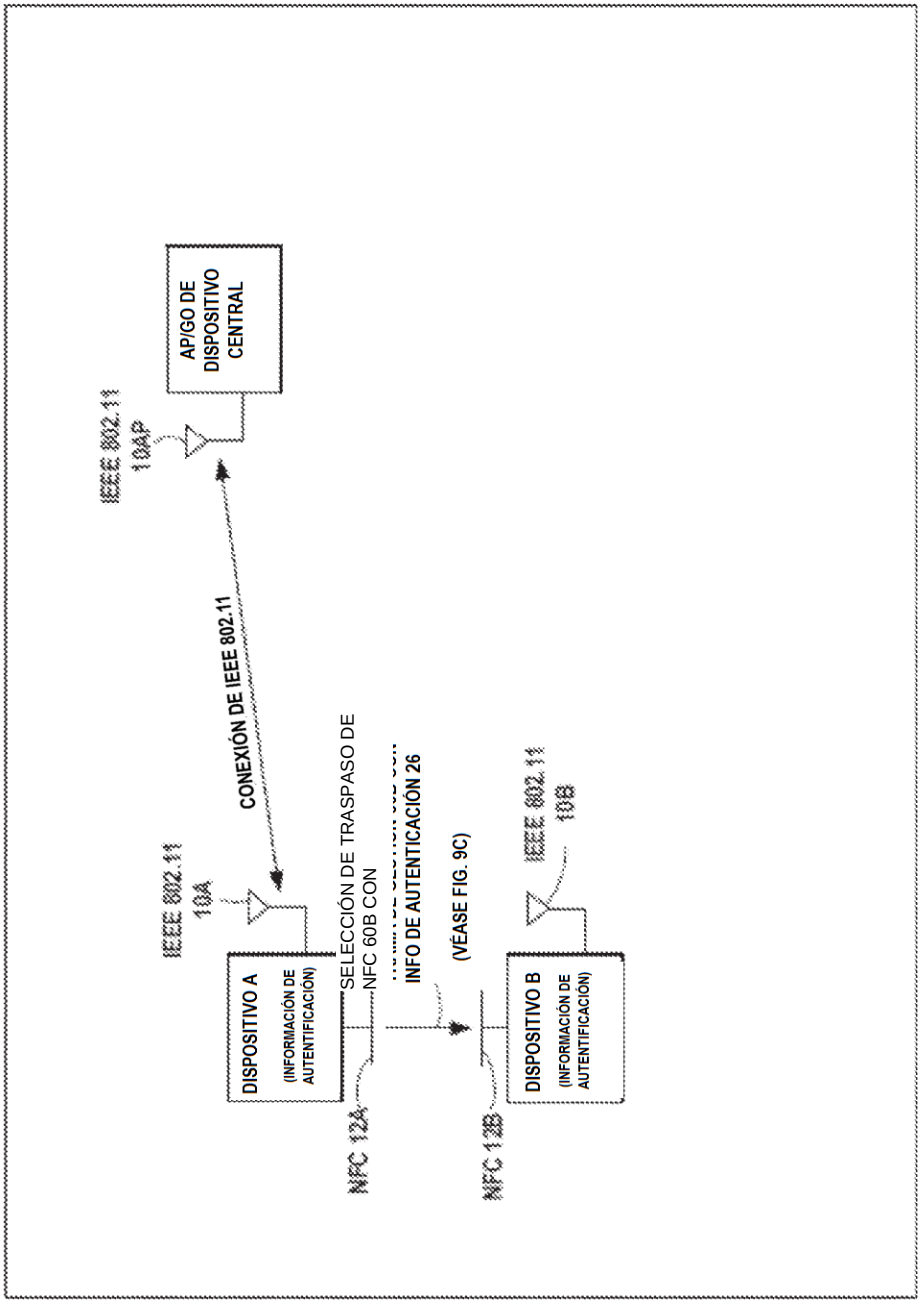

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11 10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11 10A
DISPOSITIVO A
(INFORMACIÓN DE AUTENTIFICACIÓN)
SELECCIÓN DE TRASPASO DE
NFC 60B CON
INFO DE AUTENTICACIÓN 26
(VÉASE FIG. 9C)
NFC 12A
NFC 12B
IEEE 802.11 10B
DISPOSITIVO B
(INFORMACIÓN DE AUTENTIFICACIÓN)

FIG. 8I

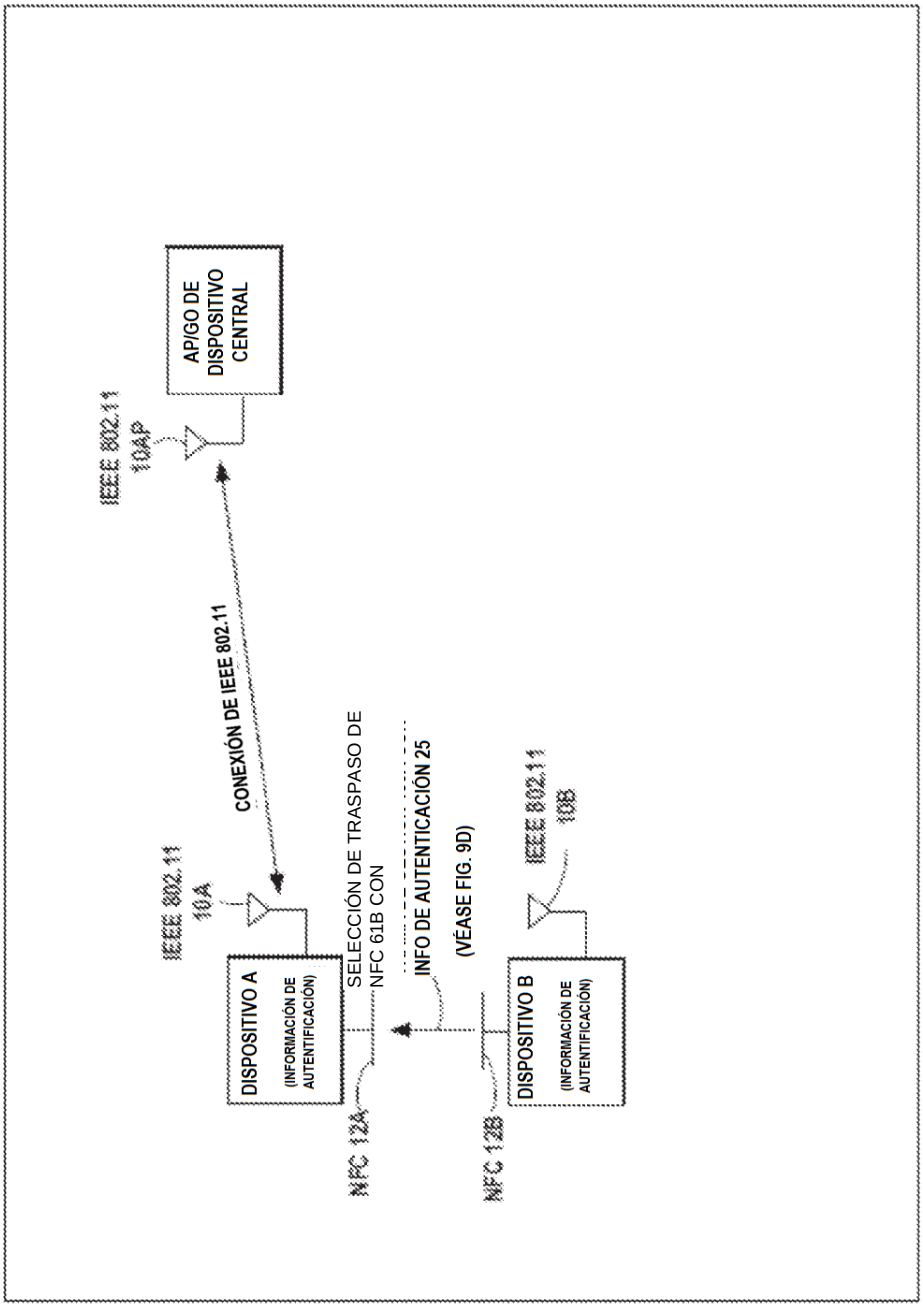

AP/GO DE DISPOSITIVO CENTRAL
IEEE 802.11
10AP
CONEXIÓN DE IEEE 802.11
IEEE 802.11
10A
DISPOSITIVO A
(INFORMACIÓN DE AUTENTIFICACIÓN)
SELECCIÓN DE TRASPASO DE NFC 61B CON
INFO DE AUTENTICACIÓN 25
(VÉASE FIG. 9D)
IEEE 802.11
10B
DISPOSITIVO B
(INFORMACIÓN DE AUTENTIFICACIÓN)
NFC 12A
NFC 12B

FIG. 8J

FIG. 9A

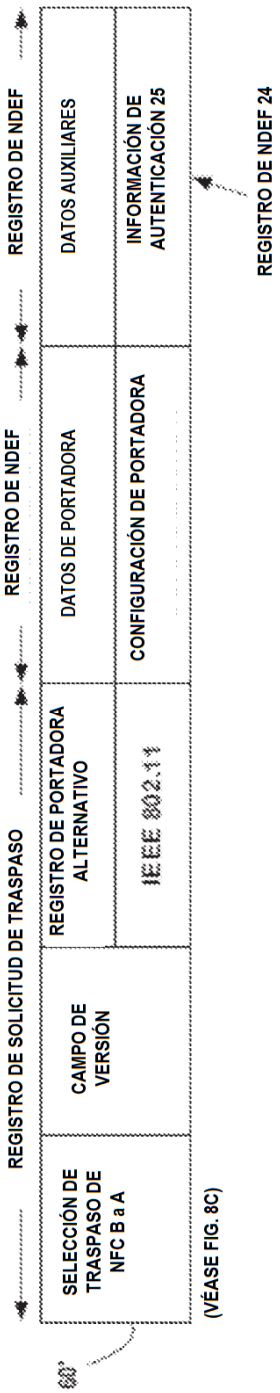

REGISTRO DE SOLICITUD DE TRASPASO
REGISTRO DE NDEF
REGISTRO DE NDEF
SELECCIÓN DE TRASPASO DE NFC B a A
CAMPO DE VERSIÓN
REGISTRO DE PORTADORA ALTERNATIVO
IEEE 802.11
DATOS DE PORTADORA
CONFIGURACIÓN DE PORTADORA
DATOS AUXILIARES
INFORMACIÓN DE AUTENTICACIÓN 25
(VÉASE FIG. 8C)
60'
REGISTRO DE NDEF 24

FIG. 9B

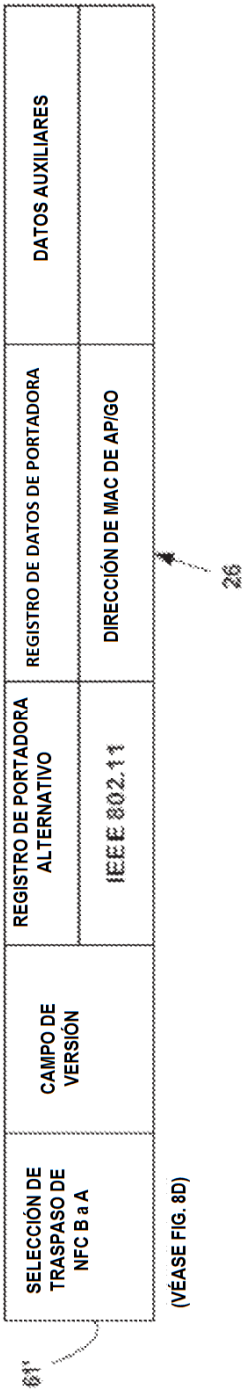

REGISTRO DE SOLICITUD DE TRASPASO
REGISTRO DE NDEF
REGISTRO DE NDEF
SELECCIÓN DE TRASPASO DE NFC B a A
CAMPO DE VERSIÓN
REGISTRO DE PORTADORA ALTERNATIVO
IEEE 802.11
REGISTRO DE DATOS DE PORTADORA
DIRECCIÓN DE MAC DE AP/GO
DATOS AUXILIARES
(VÉASE FIG. 8D)
61'
26

FIG. 9C

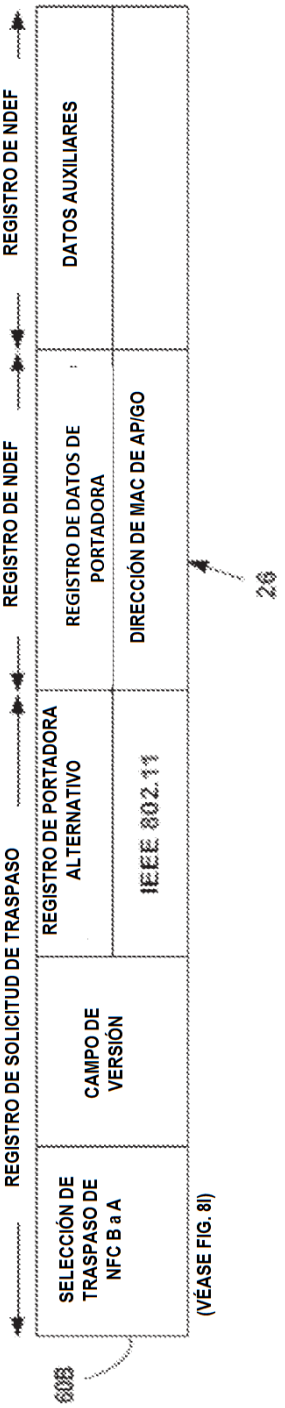
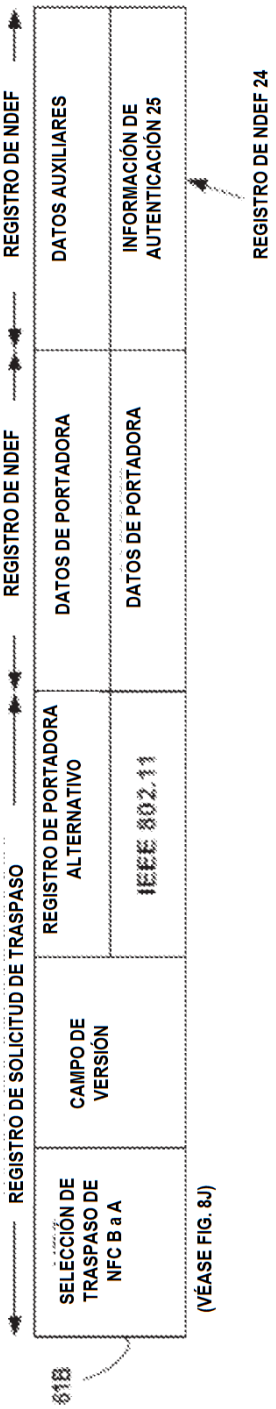

REGISTRO DE SOLICITUD DE TRASPASO
REGISTRO DE NDEF
REGISTRO DE NDEF
SELECCIÓN DE TRASPASO DE NFC B a A
CAMPO DE VERSIÓN
REGISTRO DE PORTADORA ALTERNATIVO
IEEE 802.11
REGISTRO DE DATOS DE PORTADORA
DIRECCIÓN DE MAC DE AP/GO
DATOS AUXILIARES
60B
(VÉASE FIG. 8I)
26

FIG. 9D


REGISTRO DE SOLICITUD DE TRASPASO
REGISTRO DE NDEF
REGISTRO DE NDEF
SELECCIÓN DE TRASPASO DE NFC B a A
CAMPO DE VERSIÓN
REGISTRO DE PORTADORA ALTERNATIVO
IEEE 802.11
DATOS DE PORTADORA
DATOS DE PORTADORA
DATOS AUXILIARES
INFORMACIÓN DE AUTENTICACIÓN 25
61B
(VÉASE FIG. 8J)
REGISTRO DE NDEF 24

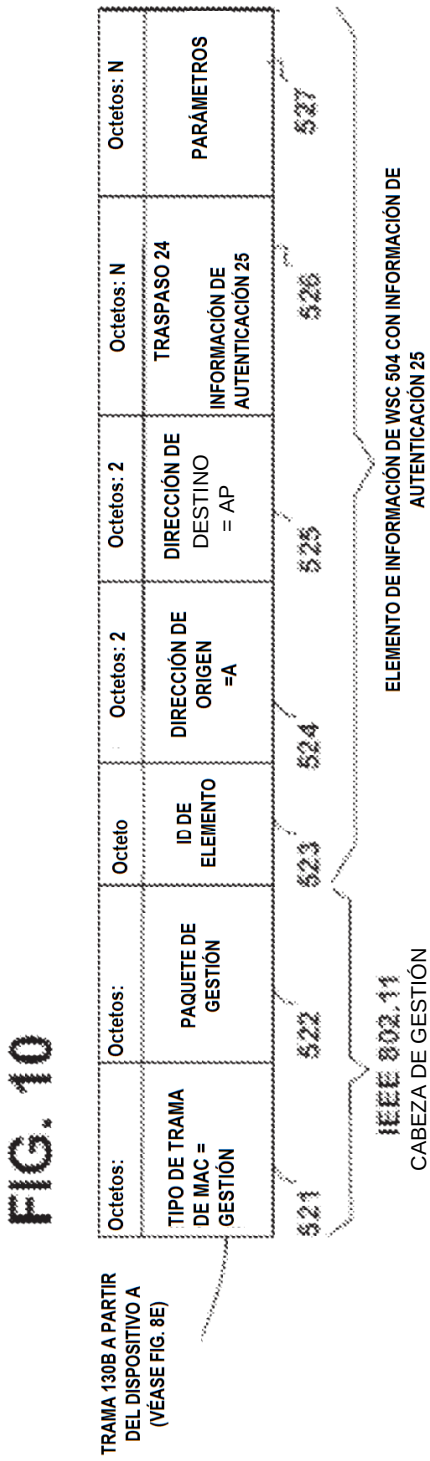


FIG. 10
TRAMA 130B A PARTIR DEL DISPOSITIVO A (VÉASE FIG. 8E)
Octetos:
TIPO DE TRAMA DE MAC = GESTIÓN
Octetos:
PAQUETE DE GESTIÓN
Octeto
ID DE ELEMENTO
Octetos: 2
DIRECCIÓN DE ORIGEN =A
Octetos: 2
DIRECCIÓN DE DESTINO = AP
Octetos: N
TRASPASO 24
INFORMACIÓN DE AUTENTICACIÓN 25
Octetos: N
PARÁMETROS
521
522
523
524
525
526
527
IEEE 802.11
CABEZA DE GESTIÓN
ELEMENTO DE INFORMACIÓN DE WSC 504 CON INFORMACIÓN DE AUTENTICACIÓN 25

FIG. 11A

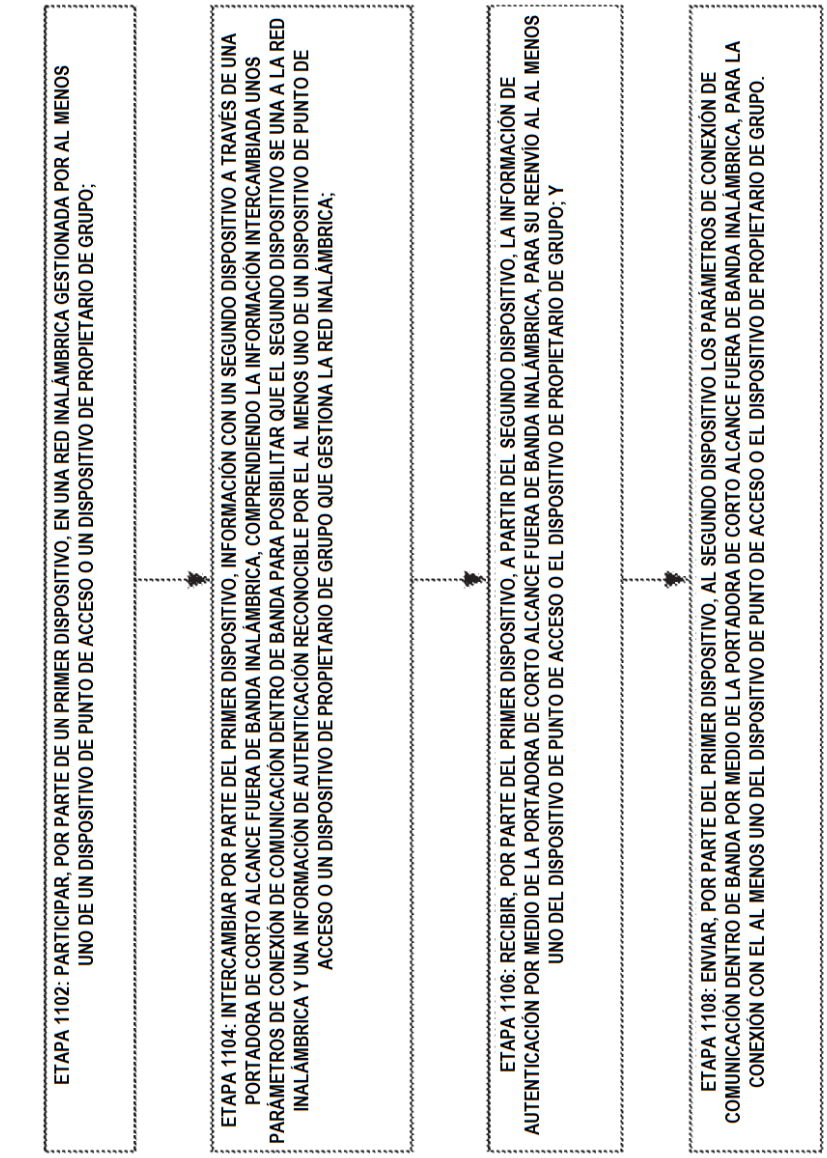

1100
ETAPA 1102: PARTICIPAR, POR PARTE DE UN PRIMER DISPOSITIVO, EN UNA RED INALÁMBRICA GESTIONADA POR AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO;
ETAPA 1104: INTERCAMBIAR POR PARTE DEL PRIMER DISPOSITIVO, INFORMACIÓN CON UN SEGUNDO DISPOSITIVO A TRAVÉS DE UNA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, COMPRENDIENDO LA INFORMACIÓN INTERCAMBIADA UNOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA PARA POSIBILITAR QUE EL SEGUNDO DISPOSITIVO SE UNA A LA RED INALÁMBRICA Y UNA INFORMACIÓN DE AUTENTICACIÓN RECONOCIBLE POR EL AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO QUE GESTIONA LA RED INALÁMBRICA;
ETAPA 1106: RECIBIR, POR PARTE DEL PRIMER DISPOSITIVO, A PARTIR DEL SEGUNDO DISPOSITIVO, LA INFORMACIÓN DE AUTENTICACIÓN POR MEDIO DE LA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, PARA SU REENVÍO AL AL MENOS UNO DEL DISPOSITIVO DE PUNTO DE ACCESO O EL DISPOSITIVO DE PROPIETARIO DE GRUPO; Y
ETAPA 1108: ENVIAR, POR PARTE DEL PRIMER DISPOSITIVO, AL SEGUNDO DISPOSITIVO LOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA POR MEDIO DE LA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, PARA LA CONEXIÓN CON EL AL MENOS UNO DEL DISPOSITIVO DE PUNTO DE ACCESO O EL DISPOSITIVO DE PROPIETARIO DE GRUPO.

FIG. 11B

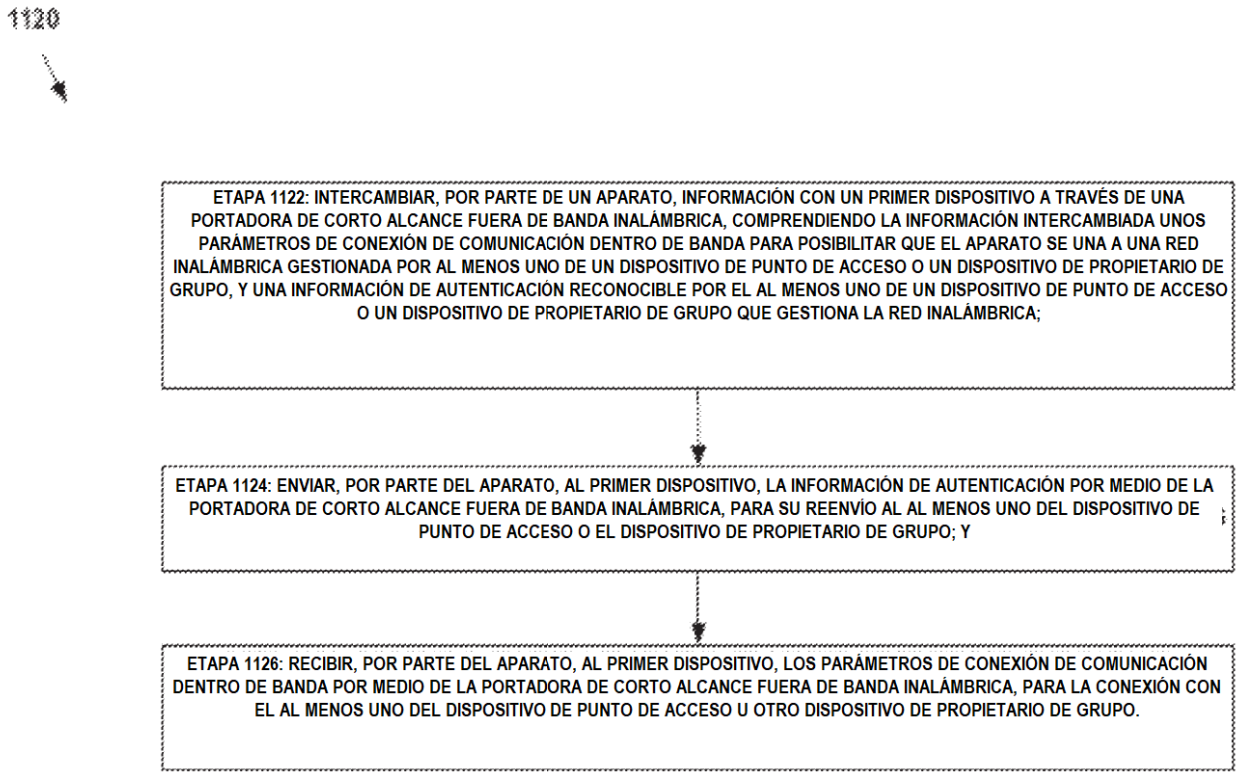
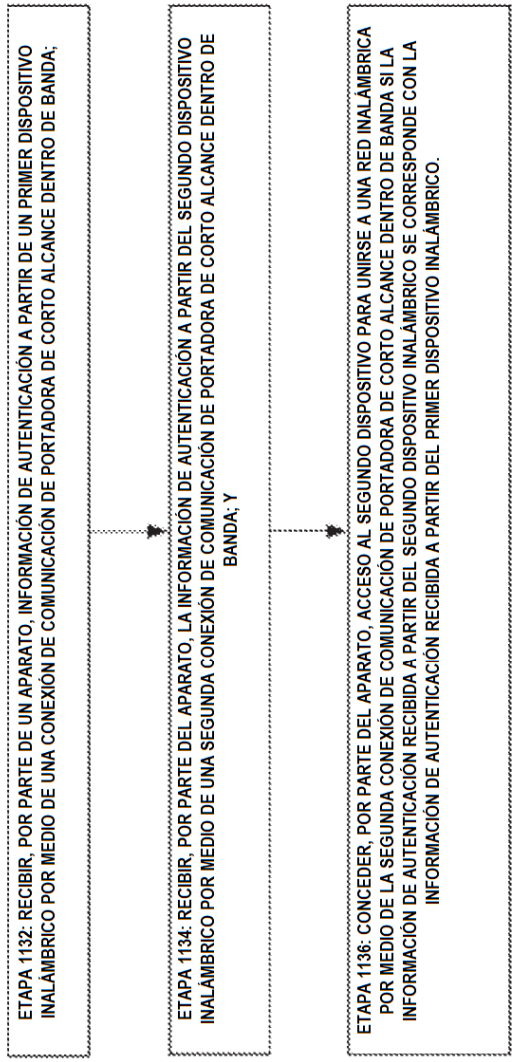

1120
ETAPA 1122: INTERCAMBIAR, POR PARTE DE UN APARATO, INFORMACIÓN CON UN PRIMER DISPOSITIVO A TRAVÉS DE UNA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, COMPRENDIENDO LA INFORMACIÓN INTERCAMBIADA UNOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA PARA POSIBILITAR QUE EL APARATO SE UNA A UNA RED INALÁMBRICA GESTIONADA POR AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO, Y UNA INFORMACIÓN DE AUTENTICACIÓN RECONOCIBLE POR EL AL MENOS UNO DE UN DISPOSITIVO DE PUNTO DE ACCESO O UN DISPOSITIVO DE PROPIETARIO DE GRUPO QUE GESTIONA LA RED INALÁMBRICA;
ETAPA 1124: ENVIAR, POR PARTE DEL APARATO, AL PRIMER DISPOSITIVO, LA INFORMACIÓN DE AUTENTICACIÓN POR MEDIO DE LA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, PARA SU REENVÍO AL AL MENOS UNO DEL DISPOSITIVO DE PUNTO DE ACCESO O EL DISPOSITIVO DE PROPIETARIO DE GRUPO; Y
ETAPA 1126: RECIBIR, POR PARTE DEL APARATO, AL PRIMER DISPOSITIVO, LOS PARÁMETROS DE CONEXIÓN DE COMUNICACIÓN DENTRO DE BANDA POR MEDIO DE LA PORTADORA DE CORTO ALCANCE FUERA DE BANDA INALÁMBRICA, PARA LA CONEXIÓN CON EL AL MENOS UNO DEL DISPOSITIVO DE PUNTO DE ACCESO U OTRO DISPOSITIVO DE PROPIETARIO DE GRUPO.

FIG. 11C

1130


ETAPA 1132: RECIBIR, POR PARTE DE UN APARATO, INFORMACIÓN DE AUTENTICACIÓN A PARTIR DE UN PRIMER DISPOSITIVO INALÁMBRICO POR MEDIO DE UNA CONEXIÓN DE COMUNICACIÓN DE PORTADORA DE CORTO ALCANCE DENTRO DE BANDA;
ETAPA 1134: RECIBIR, POR PARTE DEL APARATO, LA INFORMACIÓN DE AUTENTICACIÓN A PARTIR DEL SEGUNDO DISPOSITIVO INALÁMBRICO POR MEDIO DE UNA SEGUNDA CONEXIÓN DE COMUNICACIÓN DE PORTADORA DE CORTO ALCANCE DENTRO DE BANDA; Y
ETAPA 1136: CONCEDER, POR PARTE DEL APARATO, ACCESO AL SEGUNDO DISPOSITIVO PARA UNIRSE A UNA RED INALÁMBRICA POR MEDIO DE LA SEGUNDA CONEXIÓN DE COMUNICACIÓN DE PORTADORA DE CORTO ALCANCE DENTRO DE BANDA SI LA INFORMACIÓN DE AUTENTICACIÓN RECIBIDA A PARTIR DEL SEGUNDO DISPOSITIVO INALÁMBRICO SE CORRESPONDE CON LA INFORMACIÓN DE AUTENTICACIÓN RECIBIDA A PARTIR DEL PRIMER DISPOSITIVO INALÁMBRICO.