(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 770 699**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04L 12/24 (2006.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04W 24/02 (2009.01)
H04W 4/50 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.03.2015 PCT/US2015/018976**

(87) Fecha y número de publicación internacional: **11.09.2015 WO15134753**

(96) Fecha de presentación y número de la solicitud europea: **05.03.2015 E 15759341 (9)**

(97) Fecha y número de publicación de la concesión europea: **23.10.2019 EP 3114884**

(54) Título: **Identificación y autenticación de dispositivo en la nube**

(30) Prioridad:

07.03.2014 US 201461949918 P
26.03.2014 US 201461970763 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.07.2020

(73) Titular/es:

UBIQUITI INC. (100.0%)
685 Third Avenue, 27th Floor
New York NY 10017, US

(72) Inventor/es:

HARDY, MATTHEW;
PAOLINI-SUBRAMANYA, MAHESH;
FREI, RANDALL W. y
BAUER, JONATHAN

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Identificación y autenticación de dispositivo en la nube

Campo

Esta divulgación se refiere generalmente a identificación y autenticación de dispositivos de red. Más específicamente, esta divulgación se refiere a identificación y autenticación de dispositivos accesibles a internet a través de un entorno informático en la nube.

Antecedentes

Muchos dispositivos informáticos están equipados para comunicación a través de uno o más tipos de redes informáticas, incluyendo redes inalámbricas. Antes de que un dispositivo informático sea capaz de conectarse a una red informática inalámbrica particular, el dispositivo habitualmente puede someterse a alguna forma de aprovisionamiento de dispositivos. En este contexto, aprovisionamiento un dispositivo para conectividad de red inalámbrica puede referirse a cualquier proceso relacionado con la configuración del dispositivo para conectividad con una o más redes de dispositivo inalámbricas particulares. Por ejemplo, un dispositivo de equipo proporcionado por cliente (CPE) (por ejemplo, portátil, sobremesa, dispositivo móvil, etc.) puede aprovisionarse con ciertos ajustes de red que habilitan que el dispositivo se conecte y comunique con una red inalámbrica (o alámbrica) particular. Además, pueden añadirse componentes de red (incluyendo puntos de acceso, encaminadores inalámbricos, etc.) a redes existentes o pueden establecer su propia red, y también pueden necesitar aprovisionarse. En otros ejemplos, redes o dispositivos, incluyendo sensores y dispositivos de supervisión domésticos, seguridad y/o entretenimiento, pueden aprovisionarse con ajustes de red que habilitan que los dispositivos (por ejemplo, sensores inalámbricos, cámaras, etc.) se conecten y comuniquen con otros sensores inalámbricos y entre sí. Con el protocolo Bluetooth, algunos aspectos de aprovisionamiento pueden realizarse automáticamente usando un diálogo de mensajería inalámbrica conocido como emparejamiento. Con Wi-Fi, el aprovisionamiento puede implicar identificar un punto de acceso por nombre y proporcionar credenciales de seguridad.

Como se describe en este documento, pueden existir dificultades particulares, y beneficios de conectar una o más redes inalámbricas (y alguno o todos los dispositivos conectados a cada red "local") a un servidor remoto, por ejemplo, en la nube ("la nube"). En particular, aunque la capa adicional del servidor en la nube puede hacer el aprovisionamiento más fácil, en algunas variaciones, el potencial de riesgos de seguridad es mayor, en particular riesgo debido una disrupción remota (por ejemplo, "suplantación"), que es incluso más grave cuando los ataques pueden permitir la tremenda cantidad de control sobre la red y dispositivos individuales a través de aprovisionamiento.

Para algunos casos de uso de dispositivo, ajustes de red apropiados pueden ser desconocidos para un fabricante o proveedor de servicios asociados con un dispositivo inalámbrico y aprovisionar el dispositivo inalámbrico antes de que se proporciona a un usuario final puede no ser viable para esos usos. Además, provisional también puede incluir especificar en qué red, y qué ubicación geográfica, se situará el dispositivo. Por ejemplo, un dispositivo inalámbrico particular puede concebirse para conectividad con la red inalámbrica personal de un usuario en la casa del usuario, donde la red doméstica se conecta a punto de acceso y pasarela particulares, y la red se conecta a un servidor en la nube.

En general, aprovisionamiento puede referirse al proceso de preparar y equipar a un dispositivo o red para permitir que proporcione nuevos servicios a sus usuarios, e incluye alterar el estado de un servicio de prioridad o capacidad existente. Por ejemplo, aprovisionamiento de dispositivos puede referirse a autenticar un dispositivo de red, tal como un punto de acceso, para verificar que un usuario puede conectar y operar a través del dispositivo. En algunas variaciones, un dispositivo puede aprovisionarse para que pueda comunicarse y/o controlarse y/o supervisarse por un servidor en la nube (o software/hardware/firmware operando en un servidor remoto, por ejemplo, en la nube).

Aprovisionamiento puede configurar un sistema/red para proporcionar a un usuario verificado acceso a datos y recursos de tecnología. Por ejemplo, aprovisionamiento puede proporcionar el acceso de un usuario basándose en una identidad de usuario única y recursos apropiados para el usuario. El proceso de aprovisionamiento puede supervisar derechos de acceso y privilegios para garantizar la seguridad de un recurso y privacidad de usuario, y también puede garantizar cumplimiento y minimizar la vulnerabilidad de sistemas a penetración y abuso. El aprovisionamiento también puede reducir la cantidad de configuración personalizada.

El aprovisionamiento de "nuevos" dispositivos (por ejemplo, dispositivo nuevo de fábrica) puede ser relativamente sencillo, ya que el primer instalador/usuario del dispositivo es probable que añada legítimamente el mismo a una red (y/o capa en la nube). Sin embargo, el aprovisionamiento de dispositivos existente (por ejemplo, dispositivos que han sido operados anteriormente, por ejemplo, como parte de una red existente o bien en comunicación con un entorno informático en la nube o bien como parte de una red existente que aún no estaba en comunicación con el entorno informático en la nube. Tal dispositivo existente puede plantear un mayor riesgo porque ataques de seguridad potenciales (por ejemplo, suplantación) pueden parecerse a un nuevo aprovisionamiento legítimo de los dispositivos (por ejemplo, cuando cambian redes, ubicaciones o usuarios).

Técnicas actuales para autenticar un dispositivo de red, incluyendo CPE y puntos de acceso, pueden no abordar los problemas identificados anteriormente. Por ejemplo, la autenticación actual habitualmente depende de testigos digitales (por ejemplo, intercambiados entre un dispositivo y un servidor remoto), o requieren que un usuario proporcione únicamente la dirección (por ejemplo, dirección MAC) y/o una contraseña para autenticar el dispositivo de red y puede ser vulnerable a fraude. Los aparatos (incluyendo sistema y/o dispositivos) y método descritos en este documento pueden abordar estos problemas.

El documento US2013/0205134A1 **divulga métodos para acceder a aprovisionamiento de credenciales usando un aparato intermedio.**

El documento US2013/0340059A1 **divulga un método de seleccionar proveedores de red en los que se transmiten credenciales desde un primer dispositivo a un segundo dispositivo.**

El documento US2013/0081113A1 **divulga un método en el que un mensaje que contiene acceso se usa para establecer enlaces de comunicación entre dispositivos.**

Sumario de la divulgación

De acuerdo con la presente invención, se proporcionan métodos de aprovisionamiento automáticamente y manos libres de un dispositivo de red para comunicar con una red como se define en las reivindicaciones adjuntas.

En general, los métodos de autenticación descritos en este documento pueden incluir el intercambio independiente de una o más "claves" (mensajes secretos) entre cada uno de tres (o más) componentes, incluyendo el servidor en la nube (que puede denominarse en este documento como un entorno informático en la nube o un entorno informático remoto, o un servidor remoto, o servidor de aprovisionamiento de dispositivos, o simplemente como la "nube"), un dispositivo de red instalado o a instalarse y aprovisionarse en la red que incluye el servidor en la nube, y un dispositivo informático (que puede denominarse como un dispositivo de aprovisionamiento, un dispositivo de usuario local, un dispositivo de usuario, un dispositivo informático de usuario, un dispositivo móvil o similar). El dispositivo de red es habitualmente un dispositivo que se concibe para incluirse en la red y/o interconectado con la nube. El dispositivo de red puede denominarse como un dispositivo local, un dispositivo conectable a la red, un dispositivo de acceso inalámbrico y/o alámbrico, y puede ser cualquier CPE y/o AP y/o pasarela apropiados, o puede comunicarse con uno o más de estos.

Por ejemplo, un método de autenticación (que puede denominarse como un método de autenticación, un método de confianza, un método de probar la identidad de) de todos o algunos del dispositivo de red, nube y dispositivo informático puede comparar en general una clave que se envía de forma separada e independiente a la nube por cada uno del dispositivo o dispositivos de red y el dispositivo informático, en el que la clave se generó o bien por el dispositivo de red o bien el dispositivo informático y de forma separada e independiente intercambiada entre el dispositivo de red y el dispositivo informático antes de que envíe de forma separada e independiente la clave a la nube.

En principio, cualquiera de estos métodos podría incluir como alternativa o adicionalmente comparar una clave separada recibida por el usuario en el dispositivo informático (tanto desde la nube como el dispositivo de interconexión en red, en el que cada copia de la clave se envió independientemente y transfirió entre el dispositivo de red y nube, y generó mediante o bien el dispositivo de red o bien nube) y/o una clave separada recibida por el dispositivo de red (tanto desde la nube como el dispositivo informático, en el que las copias de la clave se enviaron independientemente al dispositivo de red después de transferirse independientemente entre la nube y el dispositivo informático y generarse por o bien la nube o bien el dispositivo informático). Por lo tanto cada concentrador (dispositivo o dispositivos de red, dispositivo informático y nube) puede validarse de forma separada o conjunta usando los métodos generales descritos en este documento.

Una vez que uno o más de los miembros de concentrador (y habitualmente la nube) verifica que las claves independientes coinciden, puede permitirse que se produzca el aprovisionamiento. En algunas variaciones, aprovisionamiento (al menos las etapas iniciales) puede combinarse con los métodos de autenticación y aparatos descritos en este documento.

En general, cualquiera de los aparatos descritos en este documento puede configurarse para realizar cualquiera (algunos o todos) de los métodos descritos en este documento. Por ejemplo, cualquiera de los aparatos (sistemas y métodos) descritos en este documento puede configurarse de modo que el aparato incluye software, hardware (por ejemplo, circuitería) y/o firmware (incluyendo un componente de circuitería), para realizar los métodos descritos en este documento.

En algunas variaciones, los métodos de autenticación descritos en este documento (por ejemplo, autenticar uno o más dispositivo o dispositivos de red, un dispositivo informático operado por usuario/instalador tal como un teléfono inteligente, y/o un servidor en la nube) puede incluir un intercambio inicial independiente de información entre dos de los concentradores (por ejemplo, el dispositivo o dispositivos de red y el dispositivo informático) usando una trayectoria

de transmisión de información que es local (por ejemplo, de modo que los dos concentradores pueden estar en proximidad, incluyendo en proximidad inmediata), y alámbrica o inalámbrica. En particular, la trayectoria de transmisión puede ser óptica (por ejemplo, lectura de un código desde el dispositivo o dispositivos de red y/o el dispositivo informático por el otro nodo). Además, esta trayectoria de transmisión es habitualmente independiente de las trayectorias de transmisión separadas entre los dos concentradores (por ejemplo, dispositivo de red y dispositivo informático) a la nube, que también pueden ser alámbricas o inalámbricas. Después del intercambio separado del código o códigos entre los dos concentradores, el código puede enviarse al tercer concentrador (por ejemplo, nube), que puede a continuación o bien responder una clave secreta que se transmite de forma separada a cualquiera (o ambos) del primer y segundo concentradores, de modo que puede leerse independientemente por o bien el primer y/o el segundo concentrador usando una trayectoria de transmisión separada que es local (por ejemplo, óptica, sónica, táctil, etc.). Para verificar la proximidad física entre los concentradores (por ejemplo, dispositivo informático y dispositivo de red), la clave puede transmitirse de vuelta a continuación al tercer concentrador (por ejemplo, nube) usando una trayectoria de transmisión diferente.

Por ejemplo, en algunas variaciones, un sistema, aparato y/o método para autenticar un dispositivo de red a través de un entorno informático en la nube puede configurarse para incluir: conectar un dispositivo de red al entorno informático en la nube; obtener un identificador único desde el dispositivo de red; enviar el identificador único al entorno informático en la nube desde un dispositivo informático; enviar una clave de autenticación desde el entorno informático en la nube al dispositivo de red a presentarse por el dispositivo de red; obtener la clave de autenticación desde el dispositivo de red; y enviar la clave de autenticación desde el dispositivo informático al entorno informático en la nube para autenticar el dispositivo de red.

Por ejemplo, conectar un dispositivo de red a un entorno informático en la nube puede incluir directamente comunicar (alámbrica o inalámbricamente) los dos dispositivos. En muchos de los ejemplos descritos en este documento, la autenticación es parte de un método y/o sistema de aprovisionamiento en el que el dispositivo de interconexión en red debe aprovisionarse antes de que pueda comunicarse completamente con el entorno en la nube. Por lo tanto, conectar el dispositivo de red y la nube puede ser una etapa inicial y/o puede incluir conexión parcial (provisional), en la que únicamente se consigue alguna (por ejemplo, mínima) conectividad. Por lo tanto, en algunas variaciones el entorno en la nube puede configurarse para comunicar provisionalmente con un dispositivo o dispositivos proporcionados. Por lo tanto, puede ser posible un simple intercambio de caracteres. Puede usarse cualquier método de conexión, pero en particular conexiones inalámbricas, por ejemplo, desde el dispositivo o dispositivos de red a la nube a través de una conexión de internet.

En general, la etapa de obtener un identificador único desde el dispositivo de red habitualmente incluye obtener el identificador único desde una trayectoria que es tanto local como independiente (independiente de cualquier conexión entre el dispositivo de red y la nube y/o el dispositivo informático y la nube). Una trayectoria local puede referirse a una trayectoria que es óptima y/o requiere una proximidad cercana para comunicar información desde la red y/o dispositivo informático. Por ejemplo, la etapa de obtener puede incluir obtener ópticamente (tomando una imagen de un código, tal como un código QR, código de barras, código alfanumérico, etc.) en uno del dispositivo de red y/o dispositivo informático. En algunas variaciones el código puede transmitirse usando una red electromagnética local (por ejemplo, RFID), u otra comunicación inalámbrica (por ejemplo, sónica, incluyendo ultrasónica).

La etapa de enviar el identificador único al entorno informático en la nube desde el dispositivo informático puede incluir transmitir el identificador único (por ejemplo, leído desde el dispositivo o dispositivos de red por el dispositivo informático, tal como un ordenador de mano o de sobremesa/teléfono inteligente) a través de una red inalámbrica que incluye una red de telecomunicaciones (por ejemplo, usando una red 4G/3G/GSM/EVDO). En general, esta red puede ser preferentemente una conexión entre el nodo (por ejemplo, el dispositivo informático) y la nube que está separada y es independiente de la conexión entre el otro nodo (el dispositivo o dispositivos de red) y la nube.

La nube puede enviar a continuación una clave de autenticación (’código secreto’) que puede generar inequívocamente para esta transacción o puede generarse de otra manera, desde el entorno informático en la nube al dispositivo de red, de modo que el dispositivo de red puede presentar la misma para detección local por el dispositivo informático. Por ejemplo, una vez recibida por el dispositivo de red (o en una variación alternativa por el dispositivo informático), el dispositivo de red puede visualizar o de otra manera proyectar localmente la misma de modo que puede leerse por el dispositivo informático. Por ejemplo, el código puede visualizare en una pantalla (o LED) para su lectura por el dispositivo informático. En algunas variaciones el código es un alfanumérico, o serie de alfanumérico (por ejemplo, secuencia de imágenes, destellos, tonos, etc.).

Una vez que el otro nodo (por ejemplo, el dispositivo informático) ha obtenido el código de autenticación (código secreto), puede enviar el mismo de vuelta a continuación al entorno informático en la nube para autenticar el dispositivo de red. Posteriormente la nube puede confiar en el dispositivo de red y el dispositivo informático, y el aprovisionamiento puede proceder (o continuar). Por ejemplo, puede descargarse software y/o firmware adicional en el uno o más dispositivos de red, puede cambiarse la configuración del dispositivo o dispositivos de red, y el dispositivo de red puede controlarse (por ejemplo, reiniciarse). Finalmente, el dispositivo o dispositivos de red pueden comunicarse directamente con la nube sin el dispositivo informático. Esto se ilustra en más detalle en este documento.

Por ejemplo, se describen en este documento métodos para autenticar un dispositivo de red a través de un entorno informático en la nube, que comprende: obtener un identificador único del dispositivo de red usando un dispositivo informático para leer el identificador único desde una superficie exterior del dispositivo de red; enviar el identificador único desde el dispositivo informático al entorno informático en la nube; transmitir una clave de autenticación desde el entorno informático en la nube al dispositivo de red, en el que el dispositivo de red presenta la clave de autenticación para detección por el dispositivo informático; obtener la clave de autenticación con el dispositivo informático desde el dispositivo de red cuando el dispositivo informático está en la presencia del dispositivo de red; enviar la clave de autenticación desde el dispositivo informático al entorno informático en la nube; y confirmar la clave de autenticación desde el dispositivo informático para autenticar el dispositivo de red.

Como se ha mencionado, puede usarse cualquier identificador único apropiado, incluyendo (pero sin limitación) un código de barras, un código QR o un código alfanumérico, que puede estar en el dispositivo de red. El dispositivo de red puede ser un punto de acceso, CPE, pasarela, etc. incluyendo sensores que forman parte de una red de detección/supervisión. En general, el dispositivo informático puede ser un dispositivo informático de mano, tal como un teléfono inteligente, tableta o similar. En algunas variaciones, el dispositivo informático es un ordenador personal

También se describen en este documento método y aparatos para aprovisionar uno o más dispositivos de red. Cualquiera de estos métodos y aparatos de aprovisionamiento también pueden incluir validación, por ejemplo, incluyendo validación de que se permite legítimamente que un dispositivo informático que ordena el aprovisionamiento aprovisione el dispositivo o dispositivos de red. En particular, cualquiera de estos aparatos puede permitir aprovisionamiento de un dispositivo de red para comunicar (por ejemplo, directamente) con un servidor en la nube.

Por ejemplo, se describen en este documento métodos implementados por ordenador, que comprenden: capturar una imagen de un código óptico fijado a un dispositivo de red, en el que el código óptico codifica un identificador único para el dispositivo; obtener una selección especificada por usuario de un sitio de dispositivo dentro del cual el dispositivo tiene que operar; determinar si el identificador único corresponde a un dispositivo conocido; y en respuesta al identificador único de código óptico que corresponde a un dispositivo conocido, aprovisionar el dispositivo para operar en el sitio de dispositivo especificado por usuario.

El identificador único puede incluir la dirección de control de acceso al medio (MAC) del dispositivo. El código óptico puede codificar la dirección MAC del dispositivo de forma encriptada. El código óptico puede codificar una cadena secreta. La cadena secreta puede codificarse de forma encriptada.

Cualquiera de estos métodos también puede incluir: en respuesta al identificador único de código óptico que corresponde a un dispositivo conocido, comunicar la cadena secreta al dispositivo para probar posesión física del dispositivo.

Por ejemplo, cualquiera de estos métodos puede incluir determinar si el identificador único de código óptico corresponde a un dispositivo conocido implica: decodificar el identificador único a partir del código óptico; y determinar si el identificador único es un identificador conocido.

El dispositivo puede incluir un punto de acceso inalámbrico para configurar el dispositivo. Aprovisionar el dispositivo puede implicar: decodificar una cadena secreta del código óptico; y enviar la cadena secreta al dispositivo como una contraseña de autenticación para acceder al punto de acceso del dispositivo. Aprovisionar el dispositivo puede implicar: decodificar una cadena secreta del código óptico; y después de acceder al punto de acceso inalámbrico, enviar la cadena secreta al dispositivo para establecer una sesión de confianza con el dispositivo.

El punto de acceso inalámbrico puede configurarse para tener un identificador de conjunto de servicios por defecto (SSID) que corresponde a un dispositivo no aprovisionado.

Cualquiera de estos métodos también puede incluir: buscar dispositivos no aprovisionados accediendo al SSID por defecto.

Por ejemplo, un medio de almacenamiento legible por ordenador no transitorio que almacena instrucciones que cuando se ejecutan por un ordenador pueden provocar que el ordenador realice un método que incluye: capturar una imagen de un código óptico fijado a un dispositivo, en el que el código óptico codifica un identificador único para el dispositivo; obtener una selección especificada por usuario de un sitio de dispositivo dentro del cual el dispositivo tiene que operar; determinar si el identificador único corresponde a un dispositivo conocido; y en respuesta al identificador único de código óptico que corresponde a un dispositivo conocido, aprovisionar el dispositivo para operar en el sitio de dispositivo especificado por usuario.

Como se ha mencionado, el identificador único puede incluir la dirección de control de acceso al medio (MAC) del dispositivo. El código óptico puede codificar la dirección MAC del dispositivo de forma encriptada. El código óptico puede codificar una cadena secreta. La cadena secreta puede codificarse de forma encriptada.

En algunas variaciones, el medio de almacenamiento se configura para: en respuesta al identificador único de código

óptico que corresponde a un dispositivo conocido, comunicar la cadena secreta al dispositivo para probar posesión física del dispositivo. Determinar si el identificador único de código óptico corresponde a un dispositivo conocido puede implicar: decodificar el identificador único a partir del código óptico; y determinar si el identificador único es un identificador conocido. El dispositivo puede incluir un punto de acceso inalámbrico para configurar el dispositivo. Aprovisionar el dispositivo puede implicar: decodificar una cadena secreta del código óptico; y enviar la cadena secreta al dispositivo como una contraseña de autenticación para acceder al punto de acceso del dispositivo. Aprovisionar el dispositivo puede implicar: decodificar una cadena secreta del código óptico; y después de acceder al punto de acceso inalámbrico, enviar la cadena secreta al dispositivo para establecer una sesión de confianza con el dispositivo.

El punto de acceso inalámbrico puede configurarse para tener un identificador de conjunto de servicios por defecto (SSID) que corresponde a un dispositivo no aprovisionado. El medio de almacenamiento puede configurarse adicionalmente para: buscar para dispositivos no aprovisionados accediendo al SSID por defecto.

También se describen en este documento aparato, que comprende: un módulo de captura de imágenes para capturar una imagen de un código óptico fijado a un dispositivo de red, en el que el código óptico codifica un identificador único para el dispositivo de red; un módulo de entrada de usuario para obtener una selección especificada por usuario de un sitio de dispositivo dentro del cual el dispositivo de red tiene que operar; un módulo de análisis para determinar si el identificador único corresponde a un dispositivo conocido; y un módulo de aprovisionamiento para aprovisionar el dispositivo de red para operar en el sitio de dispositivo especificado por usuario, en respuesta al identificador único de código óptico que corresponde a un dispositivo conocido.

El identificador único puede incluir la dirección de control de acceso al medio (MAC) del dispositivo. El código óptico puede codificar la dirección MAC del dispositivo de forma encriptada. El código óptico puede codificar una cadena secreta. La cadena secreta puede codificarse de forma encriptada. El aparato puede configurarse adicionalmente para incluir un módulo de comunicación para comunicar la cadena secreta al dispositivo para probar posesión física del dispositivo, en respuesta al identificador único de código óptico que corresponde a un dispositivo conocido. Cualquiera de los módulos descritos en este documento también puede denominarse como circuitos y puede incluir software, hardware y/o firmware configurado para realizar la función citada. Por ejemplo, un módulo de comunicación puede incluir circuitería inalámbrica y/o lógica de control para controlar circuitería inalámbrica (por ejemplo, wifi, Bluetooth, una o más radios RF, etc.). Determinar si el identificador único de código óptico corresponde a un dispositivo conocido puede incluir un módulo de análisis configurado adicionalmente para: decodificar el identificador único a partir del código óptico; y determinar si el identificador único es un identificador conocido. El módulo de análisis puede incluir circuitería y/o firmware y/o software, incluyendo uno o más comparadores adaptados/configurados para determinar si el identificador único es un identificador conocido.

El dispositivo puede ser o puede incluir un punto de acceso inalámbrico para configurar el dispositivo. Aprovisionar el dispositivo puede implicar un módulo de aprovisionamiento que se configura adicionalmente para: decodificar una cadena secreta del código óptico; y enviar la cadena secreta al dispositivo como una contraseña de autenticación para acceder al punto de acceso del dispositivo. Como se ha mencionado, el módulo de aprovisionamiento puede incluir software, hardware y/o firmware adaptados para decodificar una cadena secreta del código óptico; y enviar la cadena secreta al dispositivo como una contraseña de autenticación para acceder al punto de acceso del dispositivo. Por lo tanto, el módulo de aprovisionamiento puede incluir circuitería configurada para operar como un módulo de aprovisionamiento, y puede incluir uno o más registros configurados para mantener toda o parte de la contraseña de autenticación como se describe.

Aprovisionar el dispositivo puede incluir cualquiera de los módulos de aprovisionamiento descritos. Por ejemplo, un módulo de aprovisionamiento puede configurarse para: decodificar una cadena secreta del código óptico; y enviar la cadena secreta al dispositivo para establecer una sesión de confianza con el dispositivo, después de acceder al punto de acceso inalámbrico. Por ejemplo, el módulo de aprovisionamiento puede incluir circuitería y/o firmware y/o software adaptados para decodificar una cadena secreta del código óptico; y enviar la cadena secreta al dispositivo para establecer una sesión de confianza con el dispositivo, después de acceder al punto de acceso inalámbrico. Por ejemplo, el módulo de aprovisionamiento puede incluir circuitería que tiene uno o más comparadores (incluyendo registros (por ejemplo, memoria) y amplificadores, por ejemplo amplificadores operacionales, y/u otra circuitería) controlados (por ejemplo, guiados por software y/o firmware) para operar como el módulo de aprovisionamiento.

El punto de acceso inalámbrico puede configurarse para tener un identificador de conjunto de servicios por defecto (SSID) que corresponde a un dispositivo no aprovisionado. En algunas variaciones, el módulo de aprovisionamiento puede configurarse adicionalmente para buscar dispositivos no aprovisionados accediendo al SSID por defecto.

Breve descripción de los dibujos

Las características novedosas de la invención se exponen con particularidad en las reivindicaciones a continuación. Se obtendrá un mejor entendimiento de las características y ventajas de la presente invención mediante referencia a la siguiente descripción detallada que expone realizaciones ilustrativas, en las que se utilizan los principios de la invención, y los dibujos adjuntos de los cuales:

La Figura 1 muestra un diagrama funcional de una red que se conecta a un servidor remoto (por ejemplo, nube).

La Figura 2A es un diagrama esquemático que muestra una realización para autenticar e identificar un dispositivo de red.

La Figura 2B es un diagrama esquemático de un método de autenticación e identificación de un dispositivo de red antes o durante el aprovisionamiento.

La Figura 2C es un diagrama de flujo de la Figura 2B, que describe el método de autenticación e identificación del dispositivo.

La Figura 2D es un diagrama esquemático de otro método de autenticación e identificación de un dispositivo de red.

La Figura 2E es un diagrama de flujo de la Figura 2D, que describe el método de autenticación e identificación del dispositivo.

La Figura 3 muestra una realización de un identificador único para autenticación e identificación de un dispositivo de red.

La Figura 4 muestra una realización de una clave de autenticación presentada por una serie de luces o indicadores para autenticación e identificación de un dispositivo de red.

La Figura 5 muestra otra realización de una clave de autenticación que comprende un código presentado en un visualizador para autenticación e identificación de un dispositivo de red.

La Figura 6 es otra realización de una clave de autenticación que comprende un sonido audible para autenticación e identificación de un dispositivo de red.

Las Figuras 7A-7I ilustran otro método para autenticar un dispositivo de red.

La Figura 8 ilustra un entorno informático ilustrativo que facilita usar un dispositivo móvil para aprovisionar un dispositivo de red de acuerdo con una realización.

La Figura 9 ilustra una interfaz de usuario para aprovisionar un dispositivo de red de acuerdo con una realización.

La Figura 10 ilustra una interfaz de usuario para seleccionar un sitio de dispositivo en el que dispositivos de red se aprovisionan de acuerdo con una realización.

La Figura 11 ilustra una interfaz de usuario para proporcionar diversas opciones relacionadas con servicios a un usuario de acuerdo con una realización.

La Figura 12 ilustra una interfaz de usuario para capturar un código óptico de acuerdo con una realización.

La Figura 13 presenta un diagrama de flujo que ilustra un método para aprovisionar un dispositivo de acuerdo con una realización.

La Figura 14 presenta un diagrama de flujo que ilustra un método para seleccionar un sitio de dispositivo para aprovisionar un dispositivo de red de acuerdo con una realización.

La Figura 15 presenta un diagrama de flujo que ilustra un método para procesar un código óptico de acuerdo con una realización.

La Figura 16 presenta un diagrama de flujo que ilustra un método para configurar un dispositivo a un sitio de dispositivo, basándose en información decodificada a partir de un código óptico de acuerdo con una realización.

La Figura 17 ilustra un sistema informático de ilustrativo que facilita el aprovisionamiento de un dispositivo de red de acuerdo con una realización.

Descripción detallada

En este documento se describen aparatos (sistemas y dispositivos) y métodos para autenticación y/o aprovisionamiento de dispositivos, particularmente métodos y aparatos para autenticación y/o aprovisionamiento de sistemas y aparatos que forman parte de una red inalámbrica que está en comunicación y puede controlarse parcialmente por un servidor remoto (por ejemplo, nube). Por ejemplo, se describe en este documento aprovisionamiento de dispositivos/aparatos de red inalámbrica que incluye autenticación e identificación de los

dispositivos de red y el usuario (por ejemplo, que opera un segundo dispositivo informático y particularmente un dispositivo de telecomunicaciones móviles configurado como el segundo dispositivo informático) por el servidor remoto (en la nube). La autenticación también puede verificar el servidor remoto en la nube.

Por ejemplo, cualquiera de los aparatos y métodos descritos en este documento puede configurarse para aprovisionar uno o más dispositivos de red después y/o durante autenticación del aparato de red, un aparato controlado por usuario (por ejemplo, dispositivo informático) que supervisa el aprovisionamiento, y/o un entorno informático en la nube (por ejemplo, nube). La parte I de la descripción en este documento incluye autenticación, que puede ser particularmente útil en autenticación de uno o más (por ejemplo, todos) nodos de una red (tal como el nivel de informática en la nube de nodos, el nodo de dispositivo o dispositivos de red, y un nodo de dispositivo informático de usuario/administrador, que puede instigar o guiar aprovisionamiento).

Parte I: Autenticación

Los aparatos y métodos divulgados en este documento habitualmente requieren más de un "secreto" o código para autenticar e identificar el dispositivo de red. Estos aparatos y métodos también pueden requerir más de una trayectoria independiente para verificar/confirmar códigos de autorización. Estas técnicas pueden garantizar que un usuario confía que sus dispositivos están bajo su control, y que los dispositivos de red pueden confiar que los usuarios son quienes reivindican ser. Para propósitos de seguridad, la autenticación puede ser un prerrequisito para completar aprovisionamiento. Aunque cualquiera de los componentes del aprovisionamiento puede verificarse (por ejemplo, la nube, el dispositivo de red, un usuario/administrador de red dispositivo informático) puede ser particularmente importante verificar que el usuario/administrador que desencadena el aprovisionamiento es legítimo y/o que el dispositivo o dispositivos de red que se aprovisionan se están modificando apropiadamente, particularmente si ya eran parte de una red existente, o la misma red, y esos cambios o modificaciones se están haciendo.

La Figura 1 muestra un diagrama funcional de una red que se conecta a la internet o nube 100. La red puede incluir tanto estaciones fijas como móviles (dispositivos de red). Un módem de banda ancha 102 puede recibir y comunicar información desde la nube 100 (por ejemplo, a través de un proveedor de servicio de internet). El módem de banda ancha puede comunicarse con uno o más dispositivos de red 104, tal como puntos de acceso, a través de conexiones inalámbricas o alámbricas para proporcionar acceso de internet a dispositivos informáticos 106 en la red. Usuarios de la red pueden acceder a continuación a la internet o nube con los dispositivos informáticos. Un sistema de gestión basado en la nube para la gestión y control de los dispositivos de red 104 puede residir en la nube 100.

También se describen y muestran dispositivos informáticos 106 que pueden comprender, por ejemplo, ordenadores personales, ordenadores portátiles, tabletas, teléfonos móviles, o cualquier otro dispositivo inalámbrico o alámbrico que requieren una conexión de internet para comunicar con la nube. Estos dispositivos informáticos también pueden considerarse dispositivos de red, y pueden conectarse a los dispositivos de red de acuerdo con el protocolo intrínseco en el diseño del dispositivo, por ejemplo Wi-Fi, Bluetooth u otros. Los protocolos pueden tener diferentes velocidades o tasas de datos para transmitir y recibir datos entre el dispositivo o dispositivos informáticos 106 y los dispositivos de red 104. Durante operación inalámbrica la tasa de datos puede cambiar para reducir el impacto de cualquier interferencia o para tener en cuenta para otras condiciones. En algunas variaciones, puede usarse un dispositivo informático para guiar y/o desencadenar aprovisionamiento de uno o más dispositivo de red. Por ejemplo, puede usarse un teléfono inteligente para guiar aprovisionamiento de uno o más CPE (por ejemplo, ordenador, etc.) 106 de modo que puede comunicarse con la nube, permitiendo que la nube supervise y/o controle y/o regule la operación de la red y/o dispositivos individuales 104, 106. El aprovisionamiento puede ser necesario para que los dispositivos operen como parte de esta red que incluye nube.

En la operación, cada dispositivo informático 106 puede conectarse al dispositivo de red 104 a través de su propio protocolo que establece la tasa de comunicación para la red inalámbrica. Los dispositivos de red 104 pueden ser dispositivos de procesamiento que tienen una memoria que puede usar tanto comunicaciones inalámbricas como comunicaciones por cable como un medio de entrada-salida. Una vez que se establece la tasa de comunicación, datos desde la nube 100 pueden acoplarse a los dispositivos informáticos 106 a través de la red y los puntos de acceso 104 permitiendo que se produzcan comunicaciones.

Dispositivos de red, puntos de acceso (AP) y similares se refieren en general a dispositivos capaces de comunicación inalámbrica con dispositivos inalámbricos y capaces de o bien comunicación alámbrica o bien inalámbrica con otros dispositivos. En algunas realizaciones, dispositivos de red se comunican con dispositivos externos usando una red local. Sin embargo, no existe ningún requisito particular de que dispositivos de red tienen un enlace de comunicación alámbrico real. En algunas realizaciones, dispositivos de red podrían comunicar en su totalidad inalámbricamente.

Dispositivos informáticos, dispositivos inalámbricos, estaciones inalámbricas, estaciones móviles y similares, pueden referirse en general a dispositivos capaces de comunicación inalámbrica y/o alámbrica con dispositivos de red. En algunas realizaciones, dispositivos informáticos implementan una norma de comunicación inalámbrica tal como IEEE 802.11a, 11b, 11g u 11n. Sin embargo, en el contexto de esta divulgación, no existe ningún requisito de que se use esta norma de comunicación particular, por ejemplo, la comunicación inalámbrica podría llevarse a cabo de acuerdo con una norma distinta de 802.11, o incluso de acuerdo con una norma IEEE en su totalidad, o que todos dispositivos

informáticos usen cada uno la misma norma o incluso usen normas de comunicación inter compatibles.

En algunas realizaciones, los dispositivos de red o AP pueden incluir un sistema de gestión basado en la nube que permite que un usuario controle remotamente y cambie la operación de los dispositivos de red. Esta divulgación proporciona protocolos de autenticación e identificación que pueden ponerse en marcha para evitar uso no autorizado de la gestión basada en la nube de puntos de acceso. En algunas realizaciones, este dispositivo autenticación puede incluir el requisito de un identificador de hardware y un bloque de identificar datos de dispositivo que pueden firmarse criptográficamente por el servidor en la nube. Adicionalmente, esta divulgación proporciona métodos y protocolos para implementar dispositivo autenticación en puntos de acceso que han cambiado propiedad.

Como se describe anteriormente, una red típica puede incluir tres partes que deben validarse: la nube 100, dispositivos de red 104 y usuarios (a través de los dispositivos informáticos 106). Para que el sistema descrito anteriormente funcione correctamente, los usuarios necesitan confiar que todos los dispositivos de red 104 están bajo su control, y no están en la posesión de otra parte. Los dispositivos de red necesitan confiar que los usuarios son quienes reivindican ser (es decir, que el usuario que afirma control sobre el dispositivo es el propietario), y la nube necesita conocer quiénes son los usuarios y qué dispositivos controlan.

Como se describe en el sumario anterior, una solución para autenticar e identificar un dispositivo de red en una red, por ejemplo, cuando y/o antes de aprovisionamiento o en otros contextos, puede incluir un identificador único o contraseña dentro o sobre el dispositivo, y utilizar una transferencia de tres direcciones como se muestra en la Figura 2A. En la Figura 2A, un dispositivo de red 204, tal como un punto de acceso o CPE, puede introducirse en una red para comunicar con la nube 200. El dispositivo de red 204 puede configurarse para comunicar automáticamente con la nube para identificarse inequívocamente a sí mismo en el sistema de gestión basado en la nube 208. Esta comunicación puede abrir comunicación bidireccional entre el sistema de gestión basado en la nube 208 y el dispositivo de red 204. Sin embargo, antes de que pueda establecerse esta comunicación, puede ser deseable confirmar que la petición (por ejemplo, procedente desde un tercer dispositivo informático), el dispositivo de red, y la nube son todos legítimos.

Por ejemplo, un usuario o administrador de sistema puede obtener un identificador único 210 desde el dispositivo de red 204. El identificador único puede ser un código físicamente en el propio dispositivo, tal como un código de barras, un código de respuesta rápida (QR), un código numérico, letras escritas o un código alfanumérico, por ejemplo. La Figura 3 muestra un ejemplo de un dispositivo de red 304 que tiene un identificador único 310 que comprende un código de barras.

Haciendo referencia de nuevo a la Figura 2A, el usuario puede enviar el identificador único 210 al sistema de gestión basado en la nube 208 para indicar a la nube que el usuario está en la presencia física del dispositivo de red 204. El usuario puede enviar el identificador único al sistema de gestión basado en la nube con un dispositivo informático 206, tal como a PC, teléfono móvil o tableta con acceso a internet. Si el identificador único es un código de barras o un código QR, el código puede escanearse por el usuario con un teléfono móvil, tableta, o lector de escaneo para enviar el código al sistema de gestión basado en la nube.

Tras recibir el identificador único desde el usuario, el sistema de gestión basado en la nube 208 puede enviar al dispositivo de red 204 una clave de autenticación que puede presentarse al usuario. En la Figura 2A, el dispositivo de red incluye indicadores o visualizador 212. Sin embargo, la clave de autenticación puede difundirse al usuario a través de un visualizador en el dispositivo, una serie de luces o indicadores parpadeantes, o una señal audible, por ejemplo. La Figura 4 muestra una realización de un dispositivo de red 404 en el que la clave de autenticación de un dispositivo de red 404 se presenta al usuario en una serie de luces o indicadores parpadeantes 412. La Figura 5 muestra una realización en la que el identificador único 510 comprende un código de barras y la clave de autenticación 512 se presenta al usuario como un código alfanumérico en una pantalla de visualización. La Figura 6 ilustra otra realización en la que la clave de autenticación 612 de un dispositivo de red 604 comprende una señal audible, tal como una palabra hablada o contraseña o una serie de pitidos o ruidos.

Haciendo referencia de nuevo a la Figura 2A, el usuario puede completar la identificación y autenticación del dispositivo de red 204 enviando el código de autenticación desde el dispositivo informático 206 al sistema de gestión basado en la nube 208. El método presentado anteriormente y en la Figura 2A asegura que el usuario está en la presencia del dispositivo de red durante autenticación.

Las Figuras 2B-2C ilustran otro ejemplo de un aparato de autenticación y método de autenticación. Por ejemplo, en la Figura 2B, un dispositivo de red 2109 puede ser parte de una red existente (por ejemplo, que comprende o conectado a un AP y/o pasarela de internet) que va a modificarse o actualizarse para hablar con un servidor en la nube 2106, o puede ser un nuevo dispositivo a instalar (o un dispositivo antiguo/existente instalados en una nueva ubicación, etc.), y puede usarse un dispositivo informático de usuario 2111 (por ejemplo, por un administrador de sistema, instalador, usuario o similar) para añadir el dispositivo a la red conectada a la nube.

En este ejemplo, el dispositivo de red 2109 puede modificarse por el dispositivo de usuario 2111 después de verificación (autenticación). La Figura 2C es un flujo de proceso que ilustra un método (incluyendo etapas opcionales)

para verificar, por la nube, que el dispositivo de red 2109 y dispositivo de usuario 2111 son legítimos antes de modificación/adición del dispositivo de red 2109 para comunicar con la nube 2106. Como se ilustra en la Figura 2C, el dispositivo de red puede conectarse 2100 (o puede estar ya conectado) al entorno informático de la nube 2106. Como se ha mencionado, esta conexión puede ser provisional (significando que puede compartirse alguna información, pero puede no estar completa, por ejemplo, hasta que el aprovisionamiento está completo).

El dispositivo informático operado por un usuario 2111, puede ser, por ejemplo, un dispositivo de mano (por ejemplo, teléfono inteligente). Puede a continuación escanear/sondear el dispositivo de red 2109 para recibir un código asociado (inequívocamente asociado) con el dispositivo. Esta comunicación entre el dispositivo 2109 y el usuario 2111 puede ser local, y puede usar un canal de comunicación que es independiente y distinto de la comunicación entre el usuario y la nube y/o el dispositivo 2109 y la nube 2106. Por ejemplo, el dispositivo informático puede configurarse de modo que el usuario escanea un código 2101 (por ejemplo, código de barras, código de QR, código alfanumérico, etc.) desde el dispositivo 2109 cuando está en proximidad al dispositivo.

Posteriormente el usuario puede enviar el código recibido (por ejemplo, código de QR) a la nube 2102. Esta transmisión por el usuario 2111 a la nube 2106 puede usar una trayectoria de comunicación que es también distinta e independiente de la conexión entre el dispositivo 2109 y la nube 2106. Por ejemplo, el usuario puede contactar la nube 2106 usando una red que es diferente de una red existente a la que el dispositivo de red 2109 es o estará conectado, por ejemplo, una red telefónica tal como 3G/4G/GSM/EVDO, etc.).

El entorno informático en la nube 2106 puede transmitir a continuación una clave única 2103 (por ejemplo, clave secreta, que puede denominarse en este documento como una clave de autenticación) al dispositivo de red 2109. La clave puede ser alfanumérica, un patrón de tonos y/o destellos, etc. El dispositivo de red 2109 puede presentar a continuación (por ejemplo, visualizar, difundir localmente, etc.) la clave de autenticación de modo que puede leerse (por ejemplo, accederse localmente) por el dispositivo informático de usuario 2111. Por ejemplo, como se ha ilustrado anteriormente, el dispositivo o dispositivos de red pueden visualizar la clave en una pantalla, visualizar un patrón de luces/imágenes en la superficie exterior, una serie de tonos sónicos (incluyendo ultrasónicos) o señales, puede transmitir a través de señal de RFID local, o similar para detección 2104 por el dispositivo de usuario 2111 o un intermediario local para el dispositivo de usuario 2111 (por ejemplo, cámara que forma imagen del dispositivo 2109 que comunica con el usuario 2111, etc.). Por lo tanto, aunque la comunicación puede ser local (por ejemplo, desde el dispositivo 2109 al usuario 2111), la conexión puede ser remota y transmitirse por intermediario.

Posteriormente, el dispositivo informático de usuario 2111 puede transmitir a continuación la clave de autenticación de vuelta a la nube 2105, completar el bucle, por ejemplo, usando el canal independiente, de modo que la nube puede verificar que la identidad de todos de los nodos (dispositivo 2109 y usuario 2111).

En las Figuras 2D y 2E se ilustran un aparato y método alternativos. En este ejemplo, el usuario (por ejemplo, dispositivo informático) 2211 se conecta 2200 opcional e inicialmente a la nube 2206. El usuario a continuación abre comunicación 2201 con el dispositivo de red 2209 usando un canal/conexión local. El canal local puede ser una red local (por ejemplo, red RF, incluyendo Bluetooth, sónico (incluyendo ultrasonido), etc.). El usuario 2211 y el dispositivo 2209 pueden compartir a continuación una clave única (por ejemplo, la clave de autenticación) 2202. Por ejemplo, el dispositivo 2209 puede generar una clave de autenticación, o el usuario puede proporcionar la clave de autenticación segura. Posteriormente, el dispositivo puede enviar 2203 esta clave de autenticación a la nube 2206, usando la conexión (por ejemplo, conexión de internet inalámbrica) entre los dos. El usuario 2211 puede transmitir 2204 también e independientemente la clave a la nube 2206 usando un canal que puede estar separado y ser independiente de la conexión entre el dispositivo 2209 y la nube 2206. En algunas variaciones, la nube compara ambas claves entre sí para confirmar que coinciden e indica una coincidencia al usuario y dispositivo de red 2205. En algunas variaciones, la nube indica una coincidencia al dispositivo de red, permitiendo que continúe con aprovisionamiento (o cualquier otro procedimiento de autenticación posterior). Como alternativa, en alguna variación la nube puede pasar la clave de autenticación recibida desde el usuario 2211 al dispositivo de red 2209 para permitir que el dispositivo de red que confirme por sí mismo la autenticación.

Parte II: Aprovisionamiento

También se describe en este documento un método y aparatos para aprovisionar uno o más dispositivos (por ejemplo, dispositivos de red) para operación con un entorno informático en la nube. Como se ha mencionado, anteriormente, cualquiera de estos métodos puede incluir (pero no tiene que incluir) la autenticación descrita anteriormente, o alguna otra variación de autenticación, como parte del aprovisionamiento.

Por ejemplo, las Figuras 7A-7G ilustran un método de aprovisionamiento de un dispositivo de red en una red. En esta realización, un dispositivo de red tal como dispositivo 104 de la Figura 1 puede autenticarse con una conexión directa entre el usuario y el dispositivo. Haciendo referencia a la Figura 7A, un usuario puede abrir una app o aplicación 714 en un dispositivo informático 706 (por ejemplo, un teléfono móvil, tableta, o PC) y solicitar o iniciar aprovisionamiento de un dispositivo de red. Por ejemplo, el dispositivo informático 706 puede configurarse para autenticar un dispositivo de red en una red. En algunas realizaciones, el dispositivo informático se configura ejecutando un software de aplicación, o incluyendo de otra manera hardware y/o firmware (colectivamente denominado en este documento como

"una app"). Sin embargo, no se requiere una aplicación ("app") y el usuario puede en su lugar iniciar sesión en una app o sitio web en la nube para autenticar el dispositivo directamente.

En las Figuras 7A-7I, un procedimiento de autenticación puede embeberse en el aprovisionamiento descrito.

En la Figura 7B, el usuario puede seleccionar la opción para autenticar o "aprovisionar" al dispositivo de red (por ejemplo, un CPE cercano). El CPE cercano puede detectarse (por ejemplo, mediante una comunicación directa entre el dispositivo informático de usuario y el dispositivo de red (por ejemplo, CPE), incluyendo como se describe anteriormente, por ejemplo, explorar un código de identificación en el dispositivo, etc.). En alguna variación, la app detecta la red existente y proporciona una interfaz de usuario que permite selección de uno o más dispositivo o dispositivos de red. En la Figura 7C, el usuario puede seleccionar la ubicación (por ejemplo, el punto de acceso) en una red a la que el dispositivo de red se aprovisionará de una lista de redes (mostrada en la Figura 7C como una lista de AP). Como alternativa o adicionalmente un mapa geográfico, que muestra la relación espacial de las diferentes redes y/o conexiones entre diferentes AP. Puede mostrarse información adicional (incluyendo intensidad de señal, etc.) para ayudar al usuario en la selección de la ubicación de red. Una vez que se selecciona el dispositivo y red, la herramienta 714 puede recibir un perfil de configuración desde la nube para el dispositivo elegido, como se muestra en la Figura 7D. En otra realización, los perfiles de configuración pueden precargarse en el software de aplicación.

Obsérvese que en algunas variaciones, la identidad de uno o más de estos nodos (el usuario/dispositivo informático, el dispositivo o dispositivos de red y la nube) puede autenticarse como se describe anteriormente, en los antecedentes o explícitamente. Por ejemplo, una vez que se selecciona el dispositivo (por ejemplo, que puede incluir escanear un identificador único) pueden realizarse las etapas de las Figuras 2B-2C o 2D-2E para autenticar. Si la autenticación no "pasa", el aprovisionamiento puede detenerse. Como alternativa o adicionalmente, autenticación puede no estar completa hasta más adelante en el proceso de aprovisionamiento descrito en este ejemplo, por ejemplo, después de que se confirma una conexión entre la nube y el dispositivo de red (véase, por ejemplo, la Figura 7E), incluso en un estado preprovisional.

Haciendo referencia a las Figuras 7E-7G, el usuario puede conectar el dispositivo informático 706 al dispositivo de red 704 para autenticarse. En algunas realizaciones, el dispositivo de red 704 puede incluir su propia red Wi-Fi o inalámbrica que puede enlazarse directamente al dispositivo informático 706. En otras realizaciones, puede ser necesario conectar una pasarela inalámbrica 716 al dispositivo de red 704 para habilitar conectividad inalámbrica, como se muestra en la Figura 7E. Como alternativa, puede hacerse cualquier otro medio de conexión entre los dispositivos, incluyendo Bluetooth, por cable u otros protocolos de conexión inalámbrica. En la Figura 7F, la app 714 puede detectar el dispositivo de red 704 cuando se hace la conexión inalámbrica o alámbrica, para hacer la conexión como se muestra en la Figura 7G. En la Figura 7F, la conexión entre el dispositivo de red y el dispositivo informático puede hacerse automáticamente en la app 714. En la Figura 7G, la app puede transferir el perfil de configuración al dispositivo de red (o bien directamente desde el dispositivo de usuario o a través de la conexión de nube, en este ejemplo facilitado por una conexión usando el producto airGateway de Ubiquiti Network, Inc.).

Una vez que el perfil de configuración se ha transferido al dispositivo de red, como se muestra en la Figura 7G, el dispositivo puede conectarse a la nube (es decir, el sistema de gestión basado en la nube descrito anteriormente) para validar el perfil de configuración. El usuario también puede validarse automáticamente con la nube usando la app, como se muestra en la Figura 7H. Este ejemplo de un método de validación requiere que el usuario esté en una conexión de confianza y directa con el dispositivo de red a través de la red local proporcionada por el adaptador de airGateway (Figura 7I).

Por ejemplo, cualquiera del método descrito en este documento puede considerarse métodos de aprovisionamiento automático y manos libres de un dispositivo de red para comunicar con una red. Por ejemplo un método de aprovisionamiento automático y manos libres de un dispositivo de red para comunicar con una red puede incluir las etapas de: fijar un dispositivo de puente al dispositivo de red; transmitir inalámbricamente información acerca del dispositivo de red desde el dispositivo de puente al dispositivo informático de mano; transmitir un identificador de una segunda red seleccionada y la información acerca del dispositivo de red desde el dispositivo informático de mano a un entorno informático en la nube; transmitir información de aprovisionamiento desde el dispositivo informático de mano al dispositivo de red; aprovisionar el dispositivo de red con la información de aprovisionamiento; y eliminar el dispositivo de puente del dispositivo de red, en el que el dispositivo de red puede comunicarse con el entorno informático en la nube a través de la segunda red seleccionada directamente.

En otro ejemplo, un método de aprovisionamiento automático y manos libres de un dispositivo de red para comunicar con una red, comprendiendo el método: fijar un dispositivo de puente al dispositivo de red, en el que el dispositivo de puente forma una red ad hoc que conecta inalámbricamente el dispositivo de puente y un dispositivo informático de mano; transmitir inalámbricamente información acerca del dispositivo de red al dispositivo informático de mano; identificar una segunda red en el dispositivo informático de mano; transmitir un identificador de la segunda red y la información acerca del dispositivo de red desde el dispositivo informático de mano al entorno informático en la nube; generar información de aprovisionamiento para el dispositivo de red de modo que el dispositivo de red puede conectarse a la segunda red; transmitir la información de aprovisionamiento desde el dispositivo informático de mano al dispositivo de red; aprovisionar el dispositivo de red con la información de aprovisionamiento; y eliminar el dispositivo

de puente del dispositivo de red, en el que el dispositivo de red puede comunicarse con el entorno informático en la nube a través de la segunda red.

Cualquiera de estos métodos (o un aparato configurado para realizar cualquiera de estos métodos) puede incluir seleccionar la segunda red identificada de una lista de redes en el dispositivo informático de mano antes de transmitir el identificador de la segunda red seleccionada. Como se ha analizado anteriormente, esta lista puede estar compuesta de redes que están presentes y accesibles dentro de la ubicación geográfica que el dispositivo de red situará (por ejemplo, situará estáticamente). Por ejemplo, la lista puede incluir una lista de puntos de acceso o nodos de red con los que el dispositivo de red puede comunicarse para acceder a la red.

Información de aprovisionamiento específica para el dispositivo de red puede generarse por el dispositivo portátil, o puede generarse en el entorno informático en la nube. La información de aprovisionamiento puede ser específica al dispositivo de red, y puede incorporar la información de red a la que el dispositivo se conectará. Por ejemplo, generar información de aprovisionamiento específica para el dispositivo de red puede incluir generar la información de aprovisionamiento en el entorno informático en la nube y transferir la misma al dispositivo informático de mano.

En general, un dispositivo informático de mano puede ser cualquier dispositivo apropiado (habitualmente móvil), incluyendo en particular teléfonos inteligentes, tabletas y portátiles dispositivos. Estos dispositivos pueden ser capaces de comunicar tanto inalámbricamente (por ejemplo, a través de Bluetooth, etc.) como mediante una red de telecomunicaciones (por ejemplo, usando una red 4G/3G/GSM/EVDO). Por ejemplo, el dispositivo informático de mano puede ser un teléfono inteligente.

Los dispositivos de puente descritos en este documento pueden ser cualquier dispositivo apropiado, pero pueden incluir habitualmente dispositivos configurados para formar una red ad hoc que puede accederse inalámbricamente por el dispositivo de telecomunicaciones móvil, así como capaz de conectarse directamente al dispositivo de red (por ejemplo, el nuevo dispositivo a aprovisionar). Por ejemplo, un dispositivo de puente puede incluir un puerto de Ethernet para conectarse directamente al dispositivo de red, así como un módulo de comunicaciones (por ejemplo, módulo de comunicaciones inalámbricas, Bluetooth, etc.) que incluye una dirección IP genérica predeterminada. La dirección IP puede usarse para identificar la red ad hoc con el dispositivo informático móvil y proporcionar información y acceso entre el dispositivo informático móvil y el dispositivo de red.

En cualquiera de los métodos descritos en este documento, el dispositivo de puente puede fijarse al dispositivo de red mediante una conexión física, por ejemplo, el dispositivo de puente y el dispositivo de red pueden conectarse mediante una conexión de Ethernet. Fijar el dispositivo de puente al dispositivo de red puede incluir formar una red ad hoc con el dispositivo de puente.

En cualquiera de los métodos descritos en este documento, el dispositivo informático de mano puede identificar y conectarse inalámbricamente al dispositivo de puente. Transmitir inalámbricamente información acerca del dispositivo de red puede incluir transmitir uno o más de: un identificador de modelo de dispositivo, frecuencia operacional y ancho de banda operacional. Por ejemplo, el dispositivo de red puede transmitir un identificador que identifica la marca particular y/o modelo del dispositivo de red; cualquiera o ambos del dispositivo informático de mano y el entorno informático en la nube pueden incluir una tabla de consulta que identifica las características (por ejemplo, características operacionales) de un número de dispositivos de red. Como alternativa o adicionalmente el dispositivo de red puede transmitir una o más de estas características.

En cualquiera de estos dispositivos, la ubicación geográfica del aparato de red puede transmitirse al dispositivo informático en la nube como parte del proceso descrito en este documento. Información geográfica puede determinarse automáticamente, basándose en información proporcionada por el dispositivo de red y/o por el dispositivo informático de mano. Por ejemplo, puede proporcionarse información GPS por cualquiera o ambos del dispositivo de red y el dispositivo informático de mano. Por ejemplo, en cualquiera de estos métodos, el dispositivo informático de mano puede transmitir información de ubicación geográfica desde el dispositivo informático de mano al entorno informático en la nube. Esta información puede usarse, por ejemplo, en determinar qué redes están próximas (y, por lo tanto, el dispositivo de red puede aprovisionarse para conectarse), y/o puede asociarse con una base de datos geográfica que incluye la ubicación del nuevo aparato de red en las redes disponibles. Por lo tanto, en cualquiera de estos métodos, el entorno informático en la nube puede asociar la información de ubicación geográfica con el dispositivo de red.

Como se describe anteriormente, en telecomunicaciones o dentro de un entorno empresarial típico, un dispositivo a menudo necesita aprovisionarse antes de proporcionar servicios al dispositivo. Aprovisionar el dispositivo puede implicar añadir el dispositivo a la lista de dispositivos admisible de la red y almacenar un certificado digital en el dispositivo. Sin embargo, en la práctica, el aprovisionamiento de un nuevo dispositivo puede ser complicado y llevar mucho tiempo. Por ejemplo, durante el aprovisionamiento de dispositivos típico, un administrador de red necesita teclear manualmente los identificadores únicos del dispositivo (por ejemplo, una dirección de control de acceso al medio (MAC)) en un sistema de aprovisionamiento de dispositivos. Si el administrador de red teclea incorrectamente una porción del identificador único, el dispositivo no se unirá a la red.

Para empeorar las cosas, un usuario que tiene acceso físico al dispositivo puede no siempre ser el administrador de red que controla el sistema de aprovisionamiento de dispositivos. Esto es particularmente cierto con proveedores de servicios de Internet (ISP), en los que un usuario tiene que llamar al ISP para aprovisionar el dispositivo, y leer por teléfono la dirección MAC del dispositivo al representante del ISP. Desafortunadamente, este proceso puede llevar mucho tiempo, ya que habitualmente se deja al usuario en espera hasta que el representante está disponible para atender la llamada del usuario.

Realizaciones de la presente divulgación resuelven el problema de aprovisionamiento de un dispositivo de red para operar dentro de un sitio de dispositivo (por ejemplo, un entorno de red lógico), sin tener que introducir manualmente información de configuración en el propio dispositivo de red, o en un sistema de aprovisionamiento para el sitio de dispositivo. Por ejemplo, el usuario puede usar una aplicación de aprovisionamiento de dispositivos en un dispositivo portátil (por ejemplo, un teléfono inteligente) para capturar una imagen de un código óptico fijado en el dispositivo. La aplicación móvil puede decodificar el código óptico para obtener un identificador único para el dispositivo, así como otra información relacionada con la seguridad. Como se ha analizado anteriormente en la parte I, esto puede ser de ayuda para autenticación así como aprovisionamiento (véase, por ejemplo, la Figura 2B-2C). Este código óptico puede existir como cualquier patrón que codifica información, tal como un código de barras lineal (por ejemplo, un código de barras), código de barras (matriz) bidimensional (por ejemplo, un código de respuesta rápida (QR)) o cualquier otro patrón de codificación de datos.

Después de decodificar esta información a partir del código óptico, la aplicación de aprovisionamiento de dispositivos puede proporcionar esta información a un servidor de red que habilita servicios para el dispositivo. La aplicación de aprovisionamiento de dispositivos también puede usar la información decodificada para interactuar con el dispositivo, por ejemplo, para configurar el dispositivo para utilizar una red informática dada (por ejemplo, un punto de acceso Wi-Fi). Por lo tanto, la aplicación de aprovisionamiento de dispositivos puede automatizar operaciones de aprovisionamiento de dispositivos complicadas, requiriendo únicamente que el usuario capture una imagen de un código óptico que está fijado al dispositivo que tiene que aprovisionarse.

La Figura 8 ilustra una realización de un entorno informático 1500 que facilita usar un dispositivo móvil 1502 para aprovisionar un dispositivo de red 1504 de acuerdo con una realización. El dispositivo móvil 1502 puede incluir cualquier dispositivo que incluye o interactúa con un sensor de imagen capaz de capturar una imagen de un código óptico 1506. Por ejemplo, dispositivo móvil 1502 puede incluir un dispositivo informático autónomo, incluyendo, pero sin limitación un teléfono inteligente, un ordenador de tableta, un asistente digital personal (PDA) o un ordenador portátil.

El dispositivo móvil 1502 puede ejecutar una aplicación de software que aprovisiona al dispositivo de red 1504 escaneando el código óptico 1506 que está fijado a dispositivo de red 1504, e interactúa con un servidor de aprovisionamiento de dispositivos 1508 en una red 1510 para aprovisionar el dispositivo de red 1504. La aplicación de software puede incluir una aplicación de software nativa almacenada en dispositivo móvil 1502, o puede incluir una aplicación basada en web accesible desde un servidor web (por ejemplo, una página web alojada por el servidor de aprovisionamiento de dispositivos 1508).

El dispositivo de red 1504 puede incluir cualquier dispositivo con capacidad de red que tiene que operar dentro de una red segura, o que tiene que interactuar con otros dispositivos seguros en una red insegura. Por ejemplo, el dispositivo 1504 puede incluir un dispositivo con interfaz de sensor, un aparato con capacidad de red, un enchufe eléctrico, un interruptor de luz, un termostato o un dispositivo informático. Además, el dispositivo 1502 puede aprovisionar el dispositivo de red 1504 para operar dentro de una red informática dada (por ejemplo, un dominio de red), o para operar dentro de un "sitio" de dispositivo. El sitio de dispositivo reconoce un entorno de red lógico, que puede incluir una colección de dispositivos de red que se despliegan en una o más redes informáticas, y se agrupan para interoperar con otros dispositivos del sitio de dispositivo en la red 1510.

La red 1510 puede incluir en general cualquier tipo de canal de comunicación alámbrica y/o inalámbrica capaz de acoplar juntos nodos informáticos. La red 1510 incluye, pero sin limitación, una red de área local, una red de área extensa, una red privada, una red pública o una combinación de redes. Además, la red 1510 puede incluir una red alámbrica, una red inalámbrica o una combinación de las mismas. En algunas realizaciones, la red 1510 incluye una red basada en IP. En una realización adicional, la red 1510 incluye la internet.

En algunas realizaciones, dispositivos aprovisionados de un sitio se asignan a cada uno un certificado digital, que se usa para autenticar la comunicación del dispositivo cuando interactúan con otros dispositivos de un sitio de dispositivo común. Esto es especialmente importante cuando un sitio abarca múltiples LAN distribuidas, para evitar que dispositivos no autorizados interactúen con otros dispositivos del sitio. Esto también evita que una persona comprometa la seguridad de una organización desde dentro de la red 1510. Por ejemplo, para asignar un certificado digital al dispositivo de red 1504, el dispositivo móvil 1502 puede comunicar la información codificada en el código óptico 1506 al servidor de aprovisionamiento de dispositivos 1508, en cuyo punto servidor de aprovisionamiento de dispositivos 1508 genera el certificado digital. El dispositivo de red 1504 puede recibir a continuación el certificado digital desde el dispositivo móvil 1502, o directamente desde el servidor de aprovisionamiento de dispositivos 1508.

La Figura 9 ilustra una interfaz de usuario 1600 para aprovisionar un dispositivo de red de acuerdo con una realización. La interfaz de usuario puede implementarse en un sistema, por ejemplo, un dispositivo informático como se describe en la presente divulgación. La UI 1600 puede incluir una barra de menú superior que presenta un botón de revelación de opciones 1602, y un pulsador de menú de listado de sitios 1604. El usuario puede tocar (o de otra manera seleccionar) el botón de revelación de opciones 1602 para revelar un conjunto de opciones relacionadas con aplicaciones. Estas opciones pueden permitir que el usuario cierre sesión, puede proporcionar soporte técnico al usuario y/o puede visualizar un conjunto de notificaciones relacionadas con el sitio o relacionadas con aprovisionamiento al usuario.

El pulsador de menú de listado de sitios 1604 puede visualizar el nombre del sitio seleccionado en la actualidad (etiquetado como "sitio actual"), y visualiza un incono que indica que presionar en el pulsador 1604 revela un listado de sitios. El icono puede incluir un triángulo apuntando hacia abajo, una flecha apuntando hacia abajo o cualquier otra imagen que insinúa que puede revelarse un listado tocando en el icono. Cuando el usuario toca en el pulsador de menú de listado de sitios 1604, la UI puede actualizarse para revelar un listado de "otros sitios". Si el usuario selecciona uno de estos otros sitios (por ejemplo, tocando en una porción de la pantalla que visualiza el nombre de sitio), el sistema usa el sitio seleccionado como el "sitio actual".

La UI 1600 también puede incluir diversos segmentos de UI que proporcionan cada uno un cierto tipo de información acerca del sitio seleccionado. En algunas realizaciones, un segmento de UI puede indicar una compilación de un número de dispositivos que se han aprovisionado para operar en el "sitio" seleccionado. Por ejemplo, los segmentos de UI pueden incluir un segmento de compilación de pasarelas 1606 para visualizar una compilación de pasarelas de seguridad aprovisionadas, y un segmento de compilación de AP 1608 para visualizar una compilación de puntos de acceso aprovisionados. Estos segmentos de UI también pueden incluir un segmento de compilación de conmutadores 1610 para visualizar una compilación de conmutadores de red aprovisionados y un segmento de compilación de teléfonos 1612 para visualizar una compilación de teléfonos IP aprovisionados. También son posibles otros tipos de segmentos de UI, tal como un segmento para visualizar un número de dispositivos activos (por ejemplo, de un tipo de dispositivo dado), un número de dispositivos caídos (por ejemplo, inaccesibles o dispositivos deshabilitados), un caudal de red para un tipo de dispositivo dado (por ejemplo, un caudal actual, o un caudal agregado para una cierta ventana de tiempo), etc.

Además, la UI 1600 también puede incluir un botón de "añadir dispositivo" 1614 para añadir un dispositivo al sitio de dispositivo actual. Por ejemplo, cuando el usuario selecciona el botón 1614, el sistema puede presentar una interfaz de usuario para capturar una imagen de un código óptico. El sistema puede usar la imagen capturada para decodificar el código óptico, y para aprovisionar un dispositivo basándose en la información codificada del código óptico.

La Figura 10 ilustra una interfaz de usuario 1700 para seleccionar un sitio de dispositivo de acuerdo con una realización. La interfaz de usuario puede implementarse en un sistema, por ejemplo, un dispositivo informático como se describe en la presente divulgación. La UI 1700 visualiza un botón de revelación de opciones 1702, un pulsador de menú de listado de sitios 1704 y visualiza segmentos de UI 1708. Cuando el usuario toca en botón de revelación de opciones 1702, la UI 1700 revela un menú de opciones desde un borde predeterminado de la UI 1700 (por ejemplo, desde un borde derecho de la pantalla de visualización).

También, cuando el usuario toca en el pulsador de menú 1704, la UI 1700 revela un listado de sitios 1706 de "otros sitios". En algunas realizaciones, la UI 1700 revela el listado de sitios 1706 presentando una animación que desliza hacia abajo los segmentos de UI 1708 hasta que se revela el listado de sitios 1706 o hasta que los segmentos de UI 1708 alcanzan una posición predeterminada a lo largo de la UI 1700 (por ejemplo, hasta que los segmentos de UI 1708 no son visibles en la UI 1700). La animación puede deslizar hacia abajo los segmentos de UI 1708 a una tasa predeterminada (por ejemplo, medida en píxeles por segundo o pulgadas por segundo), o durante un intervalo de tiempo predeterminado (por ejemplo, 0,5 segundos). También, el sistema puede suavizar la animación, por ejemplo incrementando gradualmente la tasa de deslizamiento al inicio de la animación, y/o descendiendo gradualmente la tasa de deslizamiento hacia el final de la animación. Si el listado de sitios 1706 no revela la lista completa de "otros sitios" después de que se revela, la UI 1700 permite que el usuario desplace el listado de sitios 1706 para revelar otros nombres de sitios no expuestos.

La Figura 11 ilustra una interfaz de usuario 1800 para proporcionar diversas opciones relacionadas con servicios a un usuario de acuerdo con una realización. La interfaz de usuario puede implementarse en un sistema, por ejemplo, un dispositivo informático como se describe en la presente divulgación. Específicamente, la UI 1800 puede incluir un botón de revelación de opciones 1802, que cuando se presiona por el usuario, provoca que el sistema presente una animación que revela el menú de opciones 1804 (si el menú de opciones 1804 está oculto). La animación puede revelar el menú de opciones 1804 desde un borde predeterminado de la pantalla, tal como desde el borde derecho de la UI 1800. También, si el usuario toca en el botón de revelación de opciones 1802 mientras el menú de opciones 1804 está revelado, el sistema presenta una animación que desliza el menú de opciones 1804 hacia el borde predeterminado de la pantalla para ocultar menú de opciones 1804. La animación puede deslizar el menú de opciones 1804 a una tasa predeterminada o durante un intervalo de tiempo predeterminado.

El sistema también puede revelar el menú de opciones 1804 cuando el sistema detecta que el usuario ha arrastrado

su dedo desde el borde predeterminado de la UI 1800 hacia el centro de la UI 1800 (por ejemplo, arrastrando desde el borde derecho de la pantalla). También, el sistema puede ocultar el menú de opciones 1804 cuando el sistema detecta que el usuario ha arrastrado su dedo más allá del borde predeterminado de la UI 1800 (por ejemplo, arrastrando fuera del borde derecho de la pantalla).

En algunas realizaciones, el menú de opciones 1804 puede incluir un botón de cierre de sesión 1806 que el usuario puede seleccionar para cerrar sesión de una cuenta de usuario. Una vez que el usuario ha cerrado sesión, el sistema no visualiza información relacionada con los diversos sitios de dispositivo asociados con la cuenta del usuario, y no permite que el usuario aprovisione a otros dispositivos en estos sitios, hasta que el usuario inicia sesión de nuevo.

El menú de opciones 1804 también puede incluir un artículo de menú de servicio de ayuda 1808 y un artículo de menú de base de conocimiento 1810. El usuario puede seleccionar el artículo de menú de servicio de ayuda 1808 para preguntar una preguntar específica, o puede seleccionar el artículo de menú de base de conocimiento 1810 para ver un foro de información (por ejemplo, un foro de preguntas más frecuentes (FAQ)) o un foro de discusión. El menú de opciones 1804 también puede incluir un artículo de menú de notificaciones 1812, que el usuario puede seleccionar revelar notificaciones con respecto a dispositivos que se han aprovisionado en el sitio seleccionado, y/o desde cualquiera de los "otros sitios".

Recuérdese que la interfaz de usuario de la aplicación móvil proporciona un botón de "añadir dispositivo" que permite que un usuario añada un nuevo dispositivo a un sitio de dispositivo deseado (por ejemplo, usando el botón 1614 de la UI 1600). Cuando el usuario presiona el botón de "Añadir dispositivo", el sistema presenta una interfaz de usuario de captura de imagen que permite que el usuario capture un código óptico fijado a un dispositivo de red. Una vez que se captura un código óptico aceptable, el sistema puede aprovisionar el dispositivo de red usando el código óptico.

La Figura 12 ilustra una interfaz de usuario 1900 para capturar un código óptico de acuerdo con una realización. La interfaz de usuario puede implementarse en un sistema, por ejemplo, un dispositivo informático como se describe en la presente divulgación. La UI 1900 incluye un visor 1902, que visualiza imágenes capturadas por la cámara incorporada del dispositivo portátil para hacer más fácil que el usuario apunte la cámara hacia un código óptico 1906. La UI 1900 también incluye el botón de cancelar 1908, que el usuario puede usar para volver a la interfaz de usuario principal en cualquier momento (por ejemplo, la UI 1600 de la Figura 9).

En algunas realizaciones, el sistema presenta la UI 1900 deslizando el visor 1902 en vista desde un borde predeterminado de la pantalla de visualización (por ejemplo, desde el fondo de la pantalla de visualización). También, una vez que el sistema captura o decodifica un código óptico, o si el usuario toca en el botón de cancelar 1908, el sistema puede ocultar la UI 1900 deslizando el visor 1902 fuera de la vista hacia el borde predeterminado de la pantalla de visualización, o hacia cualquier otro borde (por ejemplo, un borde opuesto al borde predeterminado).

La UI 1900 también puede incluir una superposición de marco 1904 que proporciona una guía al usuario mientras el usuario está apuntando el sensor de imagen del dispositivo móvil hacia el código óptico. La superposición de marco indica una porción de visor 1902 de la que el sistema lee el código óptico. En algunas realizaciones, el sistema captura una imagen cuando detecta que el usuario ha tocado en cualquier sitio del visor 1902. El sistema debería ser capaz de decodificar el código óptico 1906 si el usuario orienta correctamente la cámara de modo que el código óptico 1906 está dentro de la superposición de marco 1904, y la imagen capturada es lo suficientemente nítida. Si el sistema no es capaz de decodificar código óptico 1906, el sistema puede informar al usuario del error, y puede presentar la UI 1900 al usuario una vez más para intentar capturar el código óptico 1906 una vez más.

La Figura 13 presenta un diagrama de flujo que ilustra un método 2000 para aprovisionar un dispositivo de red de acuerdo con una realización. Durante operación, el sistema (por ejemplo, dispositivo informático según se describe) puede presentar una interfaz de usuario que muestra información relacionada con dispositivos desplegados en uno o más sitios de dispositivo, y que permite que un usuario añada un dispositivo de red a un sitio de dispositivo (operación 2002).

En algunas realizaciones, el sistema puede recibir un evento de UI para añadir un nuevo dispositivo de red a un sitio, tal como cuando el usuario presiona en un botón de "añadir dispositivo" (operación 2004). Para añadir el dispositivo a un sitio, el sistema determina un sitio de dispositivo en el que el usuario desea añadir el nuevo dispositivo (operación 2006), y captura una imagen de un código óptico fijado al dispositivo (operación 2008). Determinar un sitio de dispositivo puede implicar, por ejemplo, lo que se divulga en conexión con la Figura 14 a continuación. El sistema puede capturar la imagen del código óptico presentando una UI de captura de imagen que el usuario puede usar para apuntar la cámara del dispositivo móvil hacia el código óptico en el dispositivo. Una vez que el usuario ha apuntado la cámara hacia el código óptico, el usuario puede tocar en la pantalla (o tocar en un icono de cámara visualizado en la pantalla) para provocar que la app de aprovisionamiento de dispositivos capture la imagen del código óptico.

El sistema analiza a continuación el código óptico para determinar si el código óptico es válido (operación 2010). Si el código óptico es válido, la aplicación de aprovisionamiento de dispositivos (y/o un servidor de aprovisionamiento de dispositivos asociado con el sitio de dispositivo seleccionado) añade el dispositivo de red al sitio de dispositivo seleccionado (operación 2012). Análisis del código óptico y adición del dispositivo de red puede implicar, por ejemplo,

lo que se divulga en conexión con la Figura 15 y la Figura 16 a continuación. Por otra parte, si el código óptico no es válido, la aplicación de aprovisionamiento de dispositivos notifica al usuario el intento fallido (operación 2014), tal como informando al usuario que el código óptico no es válido, y/o proporcionando una explicación de por qué el código óptico no es válido.

En algunas realizaciones, el sistema puede determinar si el usuario quiere intentar capturar el código óptico de nuevo (operación 2016), por ejemplo, visualizando una ventana modal que deja que el usuario elija si intentar de nuevo. Si el usuario desea intentar de nuevo, la aplicación de aprovisionamiento de dispositivos puede volver a la operación 2008 para capturar otra imagen del código óptico.

La Figura 14 presenta un diagrama de flujo que ilustra un método 2100 para seleccionar un sitio de dispositivo para aprovisionar un dispositivo de red de acuerdo con una realización. Durante operación, la aplicación de aprovisionamiento de dispositivos puede seleccionar un sitio de dispositivo anteriormente seleccionado (operación 2102). El sitio seleccionado anteriormente puede corresponder al último sitio de dispositivo en el que el usuario añadió un dispositivo, el último sitio supervisado por el usuario a través de la aplicación móvil, o puede corresponder a un sitio que el usuario ha designado anteriormente como un sitio "por defecto". La aplicación puede presentar este sitio al usuario, y puede presentar un icono de selección de sitio, que cuando se toca o selecciona de otra manera por el usuario, permite que el usuario seleccione un sitio de una lista predeterminada de sitios.

En algunas realizaciones, la aplicación de aprovisionamiento de dispositivos determina si el usuario desea seleccionar un sitio diferente (operación 2104), por ejemplo, determinando si el usuario ha seleccionado el icono de selección de sitio. Si es así, la aplicación puede presentar uno o más sitios de dispositivo existentes (por ejemplo, a partir de una lista predeterminada de sitios de dispositivo conocidos) (operación 2106), y puede recibir una selección de usuario para un sitio de dispositivo (operación 2108). La aplicación a continuación actualiza la UI de configuración de sitio para visualizar el sitio de dispositivo seleccionado por usuario (operación 2110). La UI de configuración de sitio actualizada puede visualizar información sobre su configuración (por ejemplo, una compilación de diversos tipos de dispositivos aprovisionados), y puede permitir que el usuario aprovisione un dispositivo nuevo al sitio seleccionado por usuario.

La Figura 15 presenta un diagrama de flujo que ilustra un método 2200 para procesar un código óptico de acuerdo con una realización. Durante operación, el sistema (por ejemplo, dispositivo informático según se describe) procesa el código óptico para decodificar sus componentes codificados (operación 2202), y determina si el código óptico es legible (operación 2204). Si el código óptico no es legible, el sistema notifica al usuario que el código óptico no se capturó correctamente (operación 2206), y puede abstenerse de aprovisionar el dispositivo. De otra manera, el sistema procede a decodificar un identificador de dispositivo del código óptico (operación 2208).

El sistema a continuación determina si el identificador de dispositivo es válido (operación 2210). En algunas realizaciones, el identificador de dispositivo puede no ser válido si no identifica inequívocamente un dispositivo existente (por ejemplo, no existe un dispositivo con un identificador de este tipo), o no identifica un dispositivo dentro de una lista blanca de dispositivos (por ejemplo, dispositivos que se conocen que se han comprado por una cierta organización). Si el identificador de dispositivo no es válido, el sistema puede notificar al usuario que el código óptico no es válido (operación 2212), y puede abstenerse de aprovisionar el dispositivo.

Por otra parte, si el identificador de dispositivo es válido, el sistema acepta el código óptico (operación 2214), y puede proceder para aprovisionar el dispositivo identificado.

La Figura 16 presenta un diagrama de flujo que ilustra un método 2300 para configurar un dispositivo de red a un sitio de dispositivo, basándose en información decodificada a partir de un código óptico de acuerdo con una realización. Durante operación, el sistema (por ejemplo, dispositivo informático según se describe) decodifica un identificador de dispositivo y una cadena secreta del código óptico (operación 2302) de un dispositivo de red. El identificador de dispositivo puede corresponder a una dirección de control de acceso al medio (MAC), o un identificador universalmente único (uuid) asignado por el fabricante o una entidad de aprovisionamiento (por ejemplo, un administrador para un entorno empresarial), o cualquier otro identificador único. La cadena secreta puede incluir un identificador de conjunto de servicios (SSID) para el punto de acceso por defecto de un dispositivo de red no aprovisionado, una contraseña (por ejemplo, para acceder un punto de acceso del dispositivo a través de un SSID por defecto), o cualquier otro secreto que puede usarse para probar posesión física de un dispositivo de red y/o para aprovisionar el dispositivo de red.

Como se ha mencionado anteriormente, dispositivos de red pueden incluir una radio inalámbrica para acceder a redes inalámbricas. En algunas realizaciones, un dispositivo de red no provisionado también puede usar la radio inalámbrica para proporcionar un punto de acceso inalámbrico para configurar el dispositivo. Este punto de acceso puede tener un valor de identificación de conjunto de servicio (SSID) predeterminado que se usa por cualquier dispositivo no aprovisionado, o puede tener un valor de SSID que es único para ese dispositivo. Si el valor de SSID es único para el dispositivo, el sistema puede obtener este valor de SSID a partir del código óptico. El sistema también puede obtener la contraseña del punto de acceso a partir de la cadena secreta decodificada.

El sistema a continuación accede al dispositivo de red usando el identificador de dispositivo y la cadena secreta para

probar posesión física del dispositivo (operación 2304). Mientras accede al punto de acceso del dispositivo, el sistema configura el dispositivo de red para acceder a una cierta red informática (por ejemplo, a través de otro punto de acceso), y para pertenecer a un sitio seleccionado (operación 2306). El sistema puede configurar el dispositivo de red para pertenecer a (y operar como un miembro de) el sitio seleccionado, por ejemplo, cargando un certificado digital al dispositivo de red que autentica la pertenencia del dispositivo de red al sitio seleccionado.

La Figura 17 ilustra una realización de un sistema informático (por ejemplo, un dispositivo informático de mano) 2402 que facilita aprovisionamiento un dispositivo de red de acuerdo con una realización. El sistema informático 2402 incluye un procesador 2404, una memoria 2406, un dispositivo de almacenamiento 2408 y un visualizador 2410. La memoria 2406 puede incluir una memoria volátil (por ejemplo, RAM) que sirve como una memoria gestionada y puede usarse para almacenar uno o más grupos de memoria. El visualizador 2410 puede incluir una interfaz táctil 2412 y puede usarse para visualizar un teclado en pantalla 2414. El dispositivo de almacenamiento 2408 puede almacenar el sistema operativo 2420, una aplicación móvil 2422 para aprovisionar dispositivos de red y datos 2424.

Los datos 2424 pueden incluir cualquier dato que se requiere como entrada o que se genera como salida por los métodos y/o procesos descritos en esta divulgación. Específicamente, los datos 2424 pueden incluir información con respecto a uno o más "sitios" de dispositivo, e información con respecto a dispositivos aprovisionados para estos sitios de dispositivo. Los datos 2424 también pueden incluir información de autorización para un usuario local, tal como credenciales que permiten que el usuario local vea y/o modifique las configuraciones a estos sitios de dispositivo.

El sistema informático 2402 también puede incluir un sensor de imagen 2416 y una radio inalámbrica 2418. En algunas realizaciones, la aplicación móvil 2422 puede usar el sensor de imagen 2416 para capturar una imagen de un código óptico fijado a un dispositivo de red, y decodifica el código óptico para aprovisionar el dispositivo basándose en la información decodificada. También, la aplicación móvil 2422 puede usar la radio inalámbrica 2418 para interactuar con el dispositivo de red para probar posesión física del dispositivo de red, y/o para configurar el dispositivo de red para operar como un miembro de un "sitio" deseado. Por ejemplo, la radio inalámbrica 2418 puede incluir un módulo Wi-Fi, y la aplicación móvil 2422 puede usar la información decodificada del código óptico (por ejemplo, un SSID y/o contraseña) para ganar acceso a un punto de acceso alojado por el dispositivo de red. Ganado acceso al punto de acceso del dispositivo de red usando la información decodificada, la aplicación móvil 2422 prueba que el usuario está en posesión física del dispositivo de red. También, mientras interactúa con el dispositivo de red, la aplicación móvil 2422 puede configurar el dispositivo de red para acceder a una red inalámbrica local, para asignar un "sitio" al dispositivo, y/o para realizar otras configuraciones de dispositivo.

Las estructuras de datos y código descritos en esta descripción detallada se almacenan habitualmente en un medio de almacenamiento legible por ordenador, que puede ser cualquier dispositivo o medio que puede almacenar código y/o datos para su uso por un sistema informático. El medio de almacenamiento legible por ordenador incluye, pero sin limitación, memoria volátil, memoria no volátil, dispositivos de almacenamiento magnético y óptico tal como unidades de disco, cinta magnética, CD (discos compactos), DVD (discos versátiles digitales o discos de vídeo digitales) u otros medios capaces de almacenar medios legibles por ordenador conocidos ahora o desarrollados más adelante.

Los métodos y procesos descritos en la sección de descripción detallada pueden incorporarse como código y/o datos, que pueden almacenarse en un medio de almacenamiento legible por ordenador como se describe anteriormente. Cuando un sistema informático lee y ejecuta el código y/o datos almacenados en el medio de almacenamiento legible por ordenador, el sistema informático realiza los métodos y procesos incorporados como estructuras de datos y código y almacenados dentro del medio de almacenamiento legible por ordenador.

Adicionalmente, los métodos y procesos descritos anteriormente pueden incluirse en módulos de hardware. Por ejemplo, los módulos de hardware pueden incluir, pero sin limitación, chips de circuito integrado específico de aplicación (ASIC), campos de matriz de puertas programables (FPGA) y otros dispositivos de lógica programable conocidos ahora o desarrollados más adelante. Cuando los módulos de hardware se activan, los módulos de hardware realizan los métodos y procesos incluidos dentro de los módulos de hardware.

Ejemplo

En algunos ejemplos puede configurarse o modificarse una red inalámbrica de modo que puede supervisarse y/o modificarse por un sistema de informática en la nube (por ejemplo, sistema en la nube). Un sistema en la nube puede conectarse a múltiples redes, incluyendo todos o algunos de los dispositivos (por ejemplo, AP, CPE, etc.) en las redes, y puede recibir de forma regular información acerca de la identidad, ubicación y/o rendimiento de componentes individuales y de la red o rede enlazadas al entorno informático en la nube. Por ejemplo, un entorno informático en la nube que puede usarse para supervisar, gestionar y/o regular una o más (incluyendo múltiples porciones de) redes inalámbricas puede preferirse por conveniencia en este ejemplo como un sistema "en la nube airOS". En este ejemplo, todos los dispositivos que comunican directamente con el sistema en la nube airOS pueden ejecutar un sistema operativo que es compatible con el sistema en la nube airOS, de modo que los dos pueden comunicarse de forma efectiva. La comunicación con el sistema en la nube airOS puede hacerse cuando un dispositivo se instala la primera vez, o puede hacerse como una modificación (por ejemplo, mejora) a una red existente.

Por lo tanto, en algunas variaciones, puede ser importante aprovisionar alguno o todos los dispositivo de red que comunican con el sistema en la nube airOS de modo que pueden operar de forma efectiva dentro del entorno informático en la nube airOS (por ejemplo, enviando información, incluyendo información de "impulsos" a y desde el servidor remoto, y recibiendo instrucciones desde el servidor remoto y/o configurando todos o algunos de los dispositivos para operación eficiente de la red o redes en comunicación con el sistema airOS).

Por lo tanto en algunas variaciones, para ser compatible con "nube airOS", dispositivos de red pueden estar ejecutando una versión de un sistema operativo (o software/firmware de cliente) que permite comunicación y/o control con el sistema airOS. Por lo tanto, en algunas variaciones, como parte del proceso de aprovisionamiento, cualquier dispositivo que no usa este firmware debe mejorarse para que el aprovisionamiento sea satisfactorio.

El aprovisionamiento en un ejemplo de este tipo puede realizarse como se describe anteriormente, y puede incluir cualquiera de los métodos de autenticación y aparatos descritos. Por ejemplo, en algunas variaciones, cuando un dispositivo de red nuevo o existente se añade a una red que tiene que comunicar con el sistema airOS (o cualquier otro sistema de informática en la nube) puede usarse una herramienta de descubrimiento para detectar el dispositivo de red que necesita aprovisionarse para comunicar con la nube. Por ejemplo, cuando un instalador conecta una nueva pieza de equipo (dispositivo de red) a una red, puede usarse una herramienta de descubrimiento para identificar el dispositivo no aprovisionado e instigar el aprovisionamiento. En algunas variaciones, puede añadirse un dispositivo a entorno en la nube a través de una herramienta de descubrimiento. Por ejemplo, una herramienta de descubrimiento puede ser software, firmware y/o hardware que (por ejemplo, puede ejecutarse en un dispositivo informático) permite que un usuario seleccione uno o múltiples dispositivos para añadir a la red y al entorno informático en la nube. Por ejemplo, la herramienta de descubrimiento puede permitir que el usuario introduzca información de inicio de sesión en la nube y seleccione una o más organizaciones y sitios. Esto puede ser particularmente importante ya que la nube puede usarse y compartirse por múltiples organizaciones (por ejemplo, que tienen múltiples redes) y estas redes pueden solaparse y/o estar separadas. A medida que se añaden nuevos dispositivos (dispositivos de red), pueden verificarse, inmediatamente y aprovisionarse inmediatamente o más adelante. Por ejemplo, pueden añadirse dispositivos para aprovisionamiento posterior; tras el lanzamiento del entorno en la nube, por ejemplo, nube airOS, una notificación en espera pide a la parte de aprovisionamiento que acepte [X] número de nuevos dispositivos que se han descubierto en [NOMBRE DE RED].

En algunas variaciones el dispositivo puede validarse inicialmente (por ejemplo, aprobarse). Una vez aprobado, todos los dispositivos de red pueden aparecer en la Lista de Dispositivos Identificados/No colocados en la red detectada: [NOMBRE DE RED]. Pueden aprovisionarse más adelante, por ejemplo, por el administrador de red apropiado.

En alguna variación, el sistema puede autodescubrir y/o autoaprovisionar dispositivos a medida que se añaden (o a medida que la red que ya está conectada a los dispositivos que se añaden) al sistema en la nube. Por ejemplo, un instalador puede conectar nuevo equipamiento a la red. Un dispositivo de red puede añadirse a la nube a través de firmware incorporado "Descubrimiento" e Intermediario; tras el lanzamiento del sistema en la nube (por ejemplo, airOS), el usuario puede ver una notificación en espera pidiendo a la parte de aprovisionamiento que acepte [X] número de nuevos dispositivos que se han descubierto en [NOMBRE DE RED]. Una vez aprobado, todos los dispositivos aparecen en la Lista de Dispositivos Identificados/No colocados en la red detectada: [NOMBRE DE RED].

En algunas variaciones, puede usarse un método de aprovisionamiento manualmente desde un dispositivo de red. Por ejemplo, puede no requerirse una instalación necesariamente, pero un dispositivo de red puede tener que tener acceso a internet para autenticar. Por ejemplo, una parte de aprovisionamiento (usuario) puede lanzar el sistema en la nube (por ejemplo, airOS) en un teléfono inteligente, tableta o sobremesa. En algunas variaciones, el sistema en la nube puede ser una interfaz web embebida localmente en el dispositivo. Una interfaz puede ser la misma en teléfono inteligente, tableta o sobremesa.

En algunas variaciones, el usuario puede introducir información de inicio de sesión en la nube (por ejemplo, nube airOS) y organización y/o el sitio en UI web de dispositivo. Por lo tanto, el dispositivo (dispositivo de red) debe tener acceso a internet; en algunas variaciones el dispositivo no tiene (o no tiene total) acceso a internet hasta después de aprovisionamiento. Los nuevos dispositivos de red pueden aparecer en una lista de dispositivos identificados/no colocados.

En cualquiera de estas variaciones, como se describe anteriormente, aprovisionamiento (y/o autenticación) puede realizarse usando un código (tal como un código QR). Por ejemplo, puede no requerirse instalación antes del aprovisionamiento, puede completarse antes o después del proceso de aprovisionamiento. Por ejemplo, una parte de aprovisionamiento puede lanzar el cliente de nube (por ejemplo, nube airOS) en un teléfono inteligente o tableta. El usuario puede seleccionar una organización y ubicación como se describe anteriormente. En algunas variaciones el aparato (por ejemplo, herramienta) puede incluir un escáner incorporado (por ejemplo, escáner de QR, escáner de ultrasonidos, etc.) y puede escanear el nuevo dispositivo. El dispositivo puede añadirse a continuación automáticamente a la lista de dispositivos identificados/no colocados.

Como se ha hecho referencia anteriormente, cualquiera de los métodos y aparatos descritos en este documento puede usarse para la importación en masa de dispositivos/aprovisionamiento en masa (y/o autenticación en masa) de

dispositivos, tal como dispositivos de red. Por ejemplo, a sistema en la nube (por ejemplo, nube airOS) puede permitir la migración de múltiples dispositivos (por ejemplo, dispositivos de red) en un único lote. Por ejemplo, un usuario puede introducir información de inicio de sesión en la nube, organización y/o ubicación, y migrar todos o algunos de los dispositivos existentes en su red existente o lista de dispositivos (por ejemplo, lista de anteriormente autenticados). Por ejemplo, puede aparecer dispositivos en una lista de "no colocados". Estos dispositivos pueden aprovisionarse como un lote.

En cualquiera de estas variaciones, el sistema en la nube puede conocer o inferir información de ubicación geográfica. Por lo tanto, por ejemplo, cualquiera de estos sistemas también puede comunicar esta información a/desde la nube, de modo que se coloca automáticamente en mapa geográfico, que también puede incluir información adicional (por ejemplo, intensidad de señal, interferencia, información específica de dispositivo, etc.).

Por lo tanto, cualquiera de los métodos y aparatos descritos en este documento puede permitir que un usuario aprovisione inalámbricamente desde un dispositivo informático tal como un teléfono inteligente que ejecuta una aplicación móvil ("app") que permite autenticación y/o aprovisionamiento y/o adición en el servidor en la nube, como se describe anteriormente. Por ejemplo, una aplicación móvil puede escanear en busca de dispositivos próximos (dispositivos de red) y puede seleccionar dispositivos a aprovisionar. La app puede incluir software, firmware y/o hardware en un medio no transitorio que permite que regule autenticación y/o aprovisionamiento y/o conexión a la nube. Por ejemplo, una app puede conectarse a un dispositivo de red, y añadir cada dispositivo a la cuenta en la nube (después o antes de autenticación) para aprovisionamiento inmediato o posterior. Por ejemplo en algunas variaciones, dispositivo puede aparecer una lista de dispositivos no colocados; si el dispositivo se coloca o configura con la app, la app puede automáticamente actualizar la configuración del dispositivo proporcionado por la nube (por ejemplo, aprovisionar o aprovisionar parcialmente el dispositivo). La app también puede ayudar a recopilar coordinadas de GPS para colocar geográficamente dispositivos de red en un mapa mantenido por la app y/o la nube.

También pueden describirse técnicas manuales para añadir (incluyendo autenticar y/o aprovisionar) dispositivos. Por ejemplo, pueden añadirse uno o más dispositivos de red a un entorno en la nube (por ejemplo, nube airOS). Por ejemplo, desde nube airOS, un ID único del dispositivo (por ejemplo, dirección MAC) puede añadirse manualmente a la nube, y si este ID único (por ejemplo, MAC) aparece en dispositivos no colocados cuando comunican (incluso de una manera limitada) con la nube, la nube puede solicitar/requerir autenticación y/o aprovisionamiento del aparato.

Por ejemplo, un instalador puede añadir una red de retroceso y 6 AP a una red existente para soportar una nueva base de clientes y esta red puede acoplarse al servidor en la nube, permitiendo supervisión y/o control de la red o redes por la nube, incluyendo a través de una interfaz en la nube. El instalador puede ordenar el equipo, que puede llegar a una oficina principal y aprovisionarse (por ejemplo, escáner de QR) antes de instalación in situ real. Posteriormente, el instalador puede elegir el equipo nuevo para la red de retroceso e instalación de AP en el campo. Por lo tanto, los dispositivos pueden aprobarse (autenticarse) previamente en la oficina, pero instalarse en el campo en una ubicación de instalación. El aprovisionamiento puede hacerse parcial o completamente antes de instalación de campo y los dispositivos colocados en una lista "confiable" basada en la nube para actualizar (por ejemplo, ubicación) una vez que se instalaron. Como alternativa o adicionalmente, los dispositivos pueden autenticarse (por primera vez o una segunda vez) en el sitio de instalación.

En otro ejemplo, un instalador puede tener un dispositivo móvil (dispositivo informático) para su uso en el campo; si el dispositivo se queda sin batería o si de otra manera no está disponible, el instalador puede aprovisionar la posinstalación de equipo. En un ordenador de sobremesa el instalador puede lanzar el sistema en la interfaz en la nube (por ejemplo, airOS) y notificarse que todos o algunos de los nuevos dispositivos instalados están listos para aprovisionamiento.

Cuando una característica o elemento se denomina en este documento como que está "en" otra característica o elemento, puede estar directamente en la otra característica o elemento o características y/o elementos intervinientes también pueden estar presentes. En contraste, cuando una característica o elemento se hace referencia como que está "directamente en" otra característica o elemento, no hay características o elementos intermedios presentes. Se entenderá también que, cuando una característica o elemento se hace referencia como que está "conectado", "fijado" o "acoplado" a otra característica o elemento, puede estar directamente conectado, fijado o acoplado a la otra característica o elemento o pueden estar presentes características o elementos intermedios. En contraste, cuando una característica o elemento se hace referencia como que está "directamente conectado", "directamente fijado" o "directamente acoplado" a otra característica o elemento, no hay características o elementos intermedios presentes. Aunque se describen o muestran con respecto a una realización, las características y elementos así descritos o mostrados pueden aplicarse a otras realizaciones. Se apreciará también por los expertos en la materia que las referencias a una estructura o característica que está dispuesta "adyacente" a otra característica puede tener porciones que solapan o superponen la característica adyacente.

La terminología usada en este documento es para el fin de describir realizaciones particulares únicamente y no se pretende que sea para limitar la invención. Por ejemplo, como se usa en este documento, se pretende que las formas singulares "un", "una", "el" y "la" incluyan también las formas plurales, a menos que el contexto lo indique claramente de otra manera. Se entenderá adicionalmente que los términos "comprende" y/o "comprendiendo/que comprende",

cuando se usan en esta memoria descriptiva, especifican la presencia de características indicadas, etapas, operaciones, elementos y/o componentes, pero no excluyen la presencia o adición de una o más otras características, etapas, operaciones, elementos, componentes y/o grupos de los mismos. Como se usa en este documento, el término "y/o" incluye cualquiera y todas las combinaciones de uno o más de los artículos listas asociados y puede abreviarse como "/".

Términos espacialmente relativos, tales como "debajo", "debajo de", "inferior", "sobre", "superior" y similares, pueden usarse en este documento para facilidad de descripción para describir un elemento o relación de característica a otro elemento o elementos o característica o características como se ilustra en las figuras. Se entenderá que se pretende que los términos espacialmente relativos abarquen diferentes orientaciones del dispositivo en su uso u operación además de la orientación representada en las figuras. Por ejemplo, si se invierte un dispositivo en las figuras, los elementos descritos como "debajo" o "por debajo" u otros elementos o características se orientarían entonces "sobre" los otros elementos o características. Por lo tanto, el término ilustrativo "debajo" puede abarcar tanto una orientación de sobre como de debajo. El dispositivo puede orientarse de otra manera (girarse 90 grados a otras orientaciones) y los descriptores espacialmente relativos usados en este documento interpretarse en consecuencia. De manera similar, las expresiones "hacia arriba", "hacia abajo", "vertical", "horizontal" y similares se usan en este documento para el fin de explicación únicamente a menos que se indique específicamente de otra manera.

Aunque los términos "primero" y "segundo" pueden usarse en este documento para describir diversas características/elementos (incluyendo etapas), estas características/elementos no deberían limitarse por estos términos, a no ser que el contexto indique de otra manera. Estos términos pueden usarse para distinguir una característica/elemento de otra característica/elemento. Por lo tanto, una primera característica/elemento analizado a continuación podría denominarse una segunda característica/elemento, y de manera similar, una segunda característica/elemento analizado a continuación podría denominarse una primera característica/elemento sin alejarse de los contenidos de la presente invención.

Como se usa en este documento en la memoria descriptiva y reivindicaciones, incluyendo como se usa en los ejemplos y a menos que se especifique expresamente de otra manera, todos los números pueden leerse como si se precediera la palabra "alrededor de" o "aproximadamente", incluso si el término no apareciera expresamente. La frase "alrededor de" o "aproximadamente" puede usarse cuando se describe una magnitud y/o posición para indicar que el valor y/o posición descritos se encuentra dentro de un intervalo de valores y/o posiciones esperadas razonable. Por ejemplo, un valor numérico puede tener un valor que es +/- 0,1 % del valor indicado (o intervalo de valores), +/-1 % del valor indicado (o intervalo de valores), +/- 2 % del valor indicado (o intervalo de valores), +/- 5 % del valor indicado (o intervalo de valores), +/-10 % del valor indicado (o intervalo de valores), etc. Cualquier intervalo numérico citado en este documento se concibe para incluir todos los subintervalos incluidos en el mismo.

Aunque se han descrito anteriormente diversas realizaciones ilustrativas, puede realizarse cualquiera de un número de cambios a diversas realizaciones sin alejarse del alcance de la invención como se describe mediante las reivindicaciones. Por ejemplo, el orden en el que se realizan diversas etapas de método descritas puede cambiarse a menudo en realizaciones alternativas, y en otras realizaciones alternativas una o más etapas de método pueden saltarse completamente. Pueden incluirse características opcionales de diversas realizaciones de dispositivo y sistema en algunas realizaciones y no en otras. Por lo tanto, la descripción anterior se proporciona principalmente para propósitos ilustrativos y no debería interpretarse para limitar el alcance de la invención como se expone en las reivindicaciones.

Los ejemplos e ilustraciones incluidos en este documento muestran, por medio de ilustración y no de limitación, realizaciones específicas en las que puede ponerse en práctica la materia objeto. Como se ha mencionado, pueden utilizarse y derivarse otras realizaciones a partir de las mismas, de manera que pueden realizarse sustituciones y cambios estructurales sin alejarse del alcance de esta divulgación. Se puede hacer referencia en este documento a tales realizaciones de la materia objeto inventiva, individual o colectivamente, mediante la expresión "invención" meramente por razones de conveniencia y sin tener por objeto limitar voluntariamente el alcance de la presente solicitud a invención o concepto inventivo individual alguno si, de hecho, se divulga más de uno. Por lo tanto, aunque en este documento se han ilustrado y descrito realizaciones específicas, que cualquier disposición calculada para lograr el mismo fin puede sustituir a las realizaciones específicas mostradas. Esta divulgación se concibe para cubrir todas y cada una de las adaptaciones o variaciones de diversas realizaciones. Algunas combinaciones de las realizaciones anteriores, y otras realizaciones no descritas específicamente en este documento, serán evidentes a los expertos en la materia tras la revisión de la descripción anterior.

REIVINDICACIONES

1. Un método de aprovisionamiento automáticamente de un dispositivo de red para comunicar con una red, comprendiendo el método:

fijar un dispositivo de puente al dispositivo de red, en el que el dispositivo de puente forma una red ad hoc que conecta inalámbricamente el dispositivo de puente a un dispositivo informático de mano;
transmitir inalámbricamente información acerca del dispositivo de red desde el dispositivo de puente al dispositivo informático de mano;
identificar una segunda red, diferente de la red ad hoc en el dispositivo informático de mano; y
transmitir un identificador de la segunda red identificada y la información acerca del dispositivo de red desde el dispositivo informático de mano a un entorno informático en la nube;
generar información de aprovisionamiento en el entorno informático en la nube para el dispositivo de red de modo que el dispositivo de red puede conectarse a la segunda red;
transmitir la información de aprovisionamiento desde el dispositivo informático de mano al dispositivo de red;
aprovisionar el dispositivo de red con la información de aprovisionamiento; y
eliminar el dispositivo de puente del dispositivo de red, en el que el dispositivo de red se habilita para comunicar con el entorno informático en la nube a través de la segunda red identificada directamente.

2. El método de la reivindicación 1, comprendiendo adicionalmente seleccionar la segunda red identificada de una lista de redes en el dispositivo informático de mano antes de transmitir el identificador de la segunda red seleccionada.

3. El método de la reivindicación 1, comprendiendo adicionalmente generar información de aprovisionamiento específica para el dispositivo de red.

4. El método de la reivindicación 1, comprendiendo adicionalmente fijar el dispositivo de puente en el que el dispositivo de puente y el dispositivo de red se conectan mediante una conexión de Ethernet.

5. El método de la reivindicación 1, en el que generar información de aprovisionamiento específica para el dispositivo de red comprende generar la información de aprovisionamiento en el entorno informático en la nube y transferir la misma al dispositivo informático de mano.

6. El método de la reivindicación 1, en el que el dispositivo informático de mano es un teléfono inteligente.

7. El método de la reivindicación 1, comprendiendo adicionalmente identificar y conectar inalámbricamente al dispositivo de puente con el dispositivo informático de mano.

8. El método de la reivindicación 1, en el que transmitir inalámbricamente información acerca del dispositivo de red comprende transmitir uno o más de: un identificador de modelo de dispositivo, frecuencia operacional y ancho de banda operacional.

9. El método de la reivindicación 1, comprendiendo adicionalmente transmitir información de ubicación geográfica desde el dispositivo informático de mano al entorno informático en la nube, y asociar la información de ubicación geográfica con el dispositivo de red en el entorno informático en la nube.

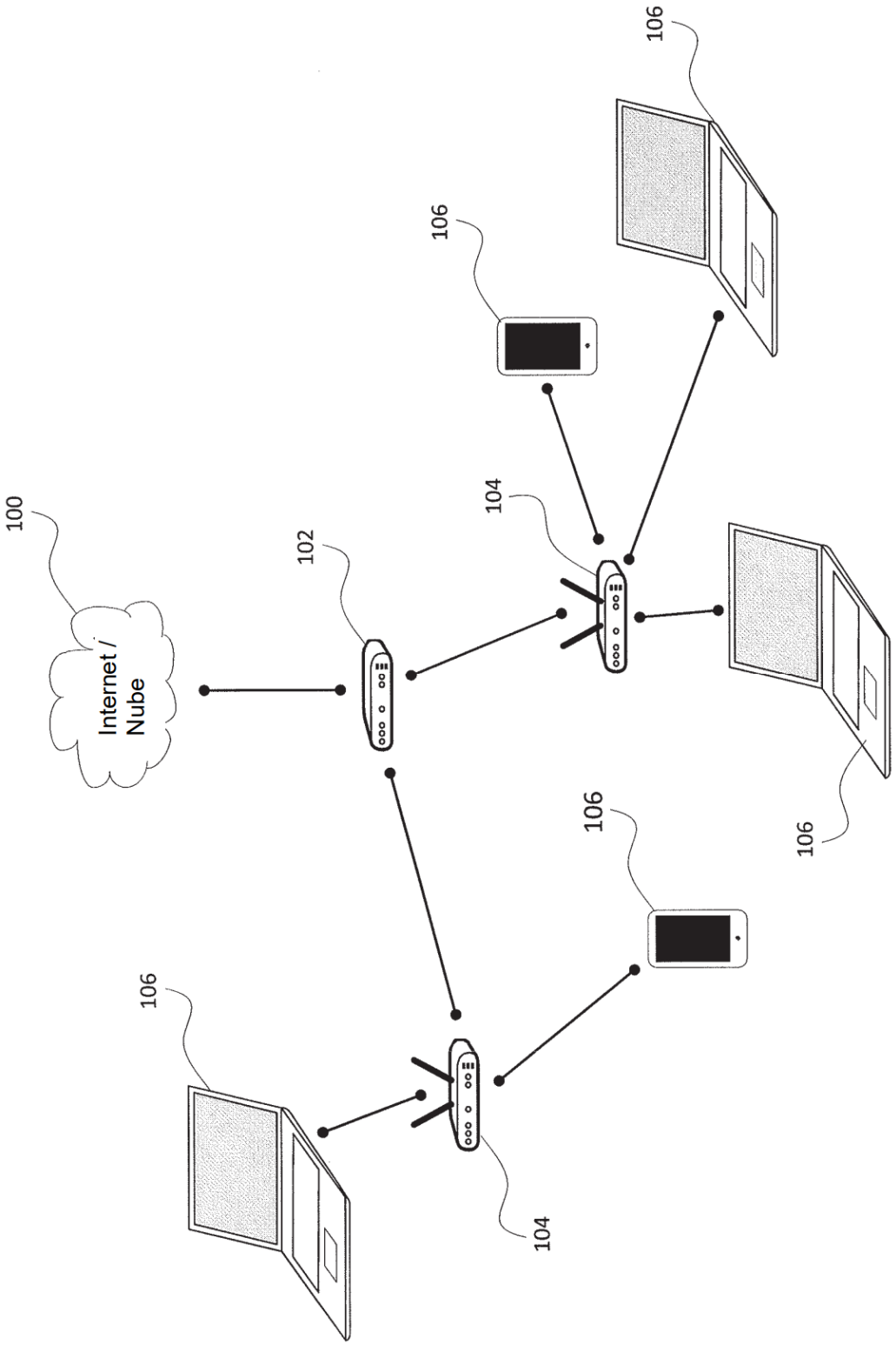

FIG. 1

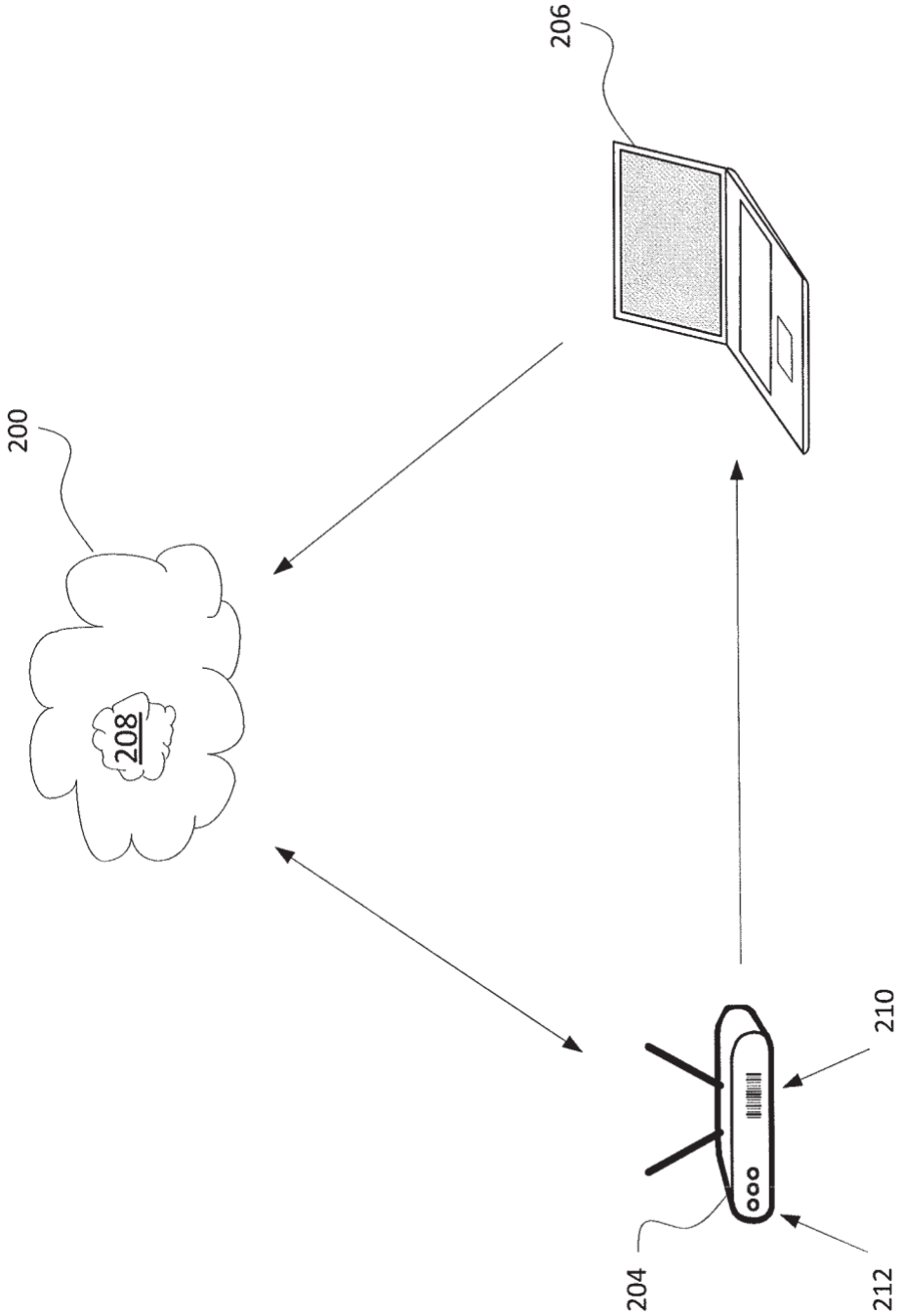

FIG. 2A

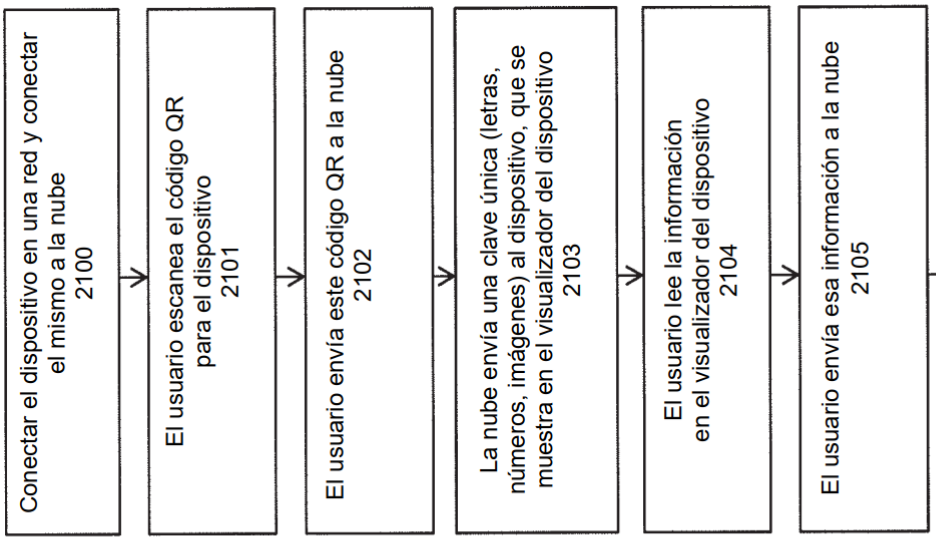
Conectar el dispositivo en una red y conectar el mismo a la nube 2100
El usuario escanea el código QR para el dispositivo 2101
El usuario envía este código QR a la nube 2102
La nube envía una clave única (letras, números, imágenes) al dispositivo, que se muestra en el visualizador del dispositivo 2103
El usuario lee la información en el visualizador del dispositivo 2104
El usuario envía esa información a la nube 2105

FIG. 2C

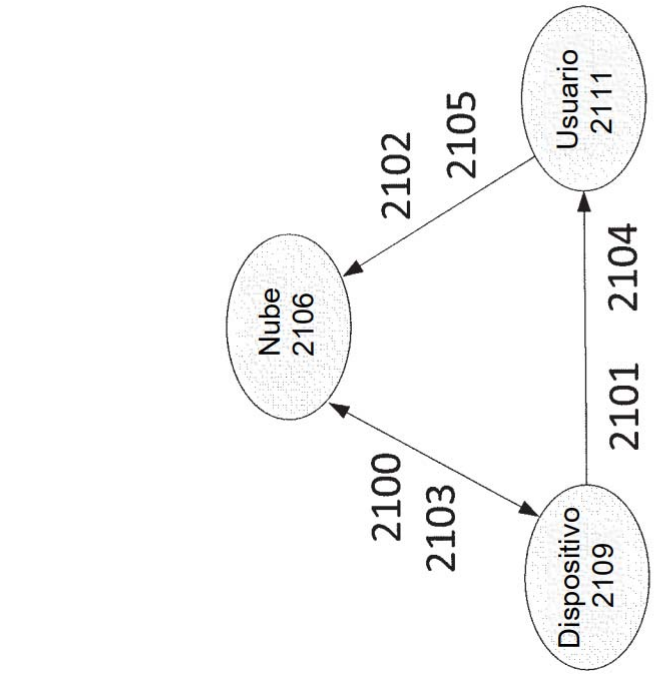
Nube 2106
Usuario 2111
Dispositivo 2109
2100
2103
2101
2102
2104
2105

FIG. 2B

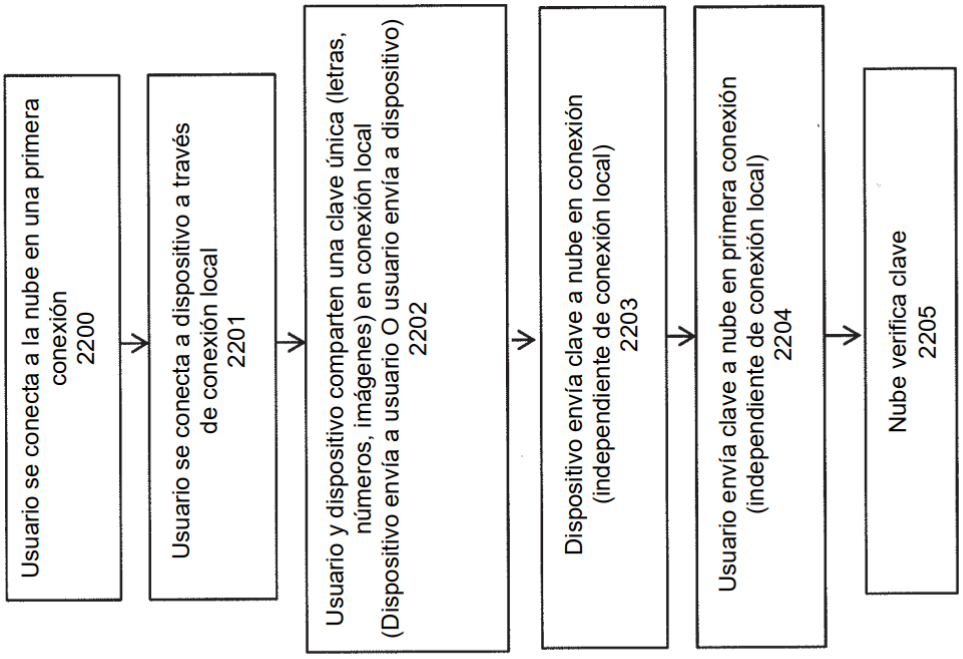
Usuario se conecta a la nube en una primera conexión 2200
Usuario se conecta a dispositivo a través de conexión local 2201
Usuario y dispositivo comparten una clave única (letras, números, imágenes) en conexión local (Dispositivo envía a usuario O usuario envía a dispositivo) 2202
Dispositivo envía clave a nube en conexión (independiente de conexión local) 2203
Usuario envía clave a nube en primera conexión (independiente de conexión local) 2204
Nube verifica clave 2205

FIG. 2E

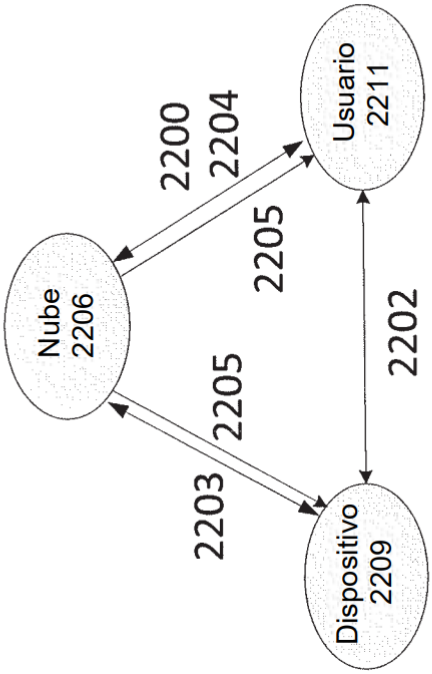
Nube 2206
Usuario 2211
Dispositivo 2209
2200
2204
2205
2205
2203
2202
2201

FIG. 2D

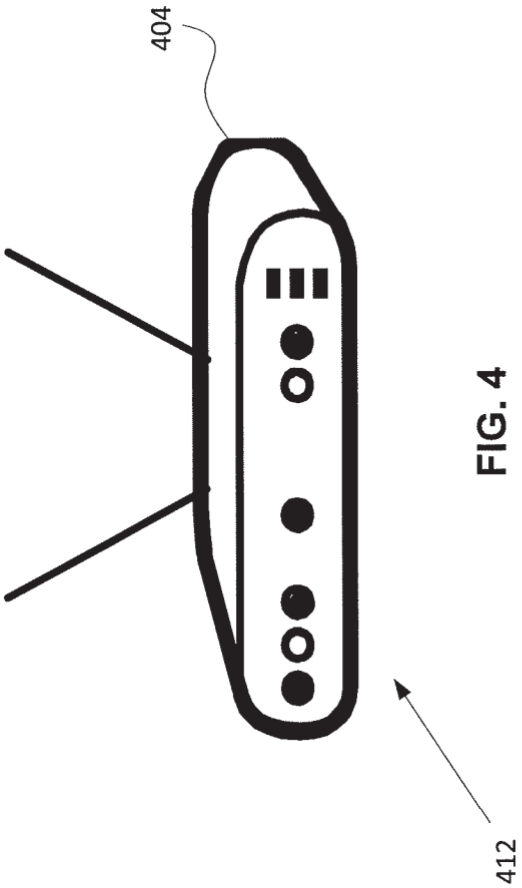

FIG. 4

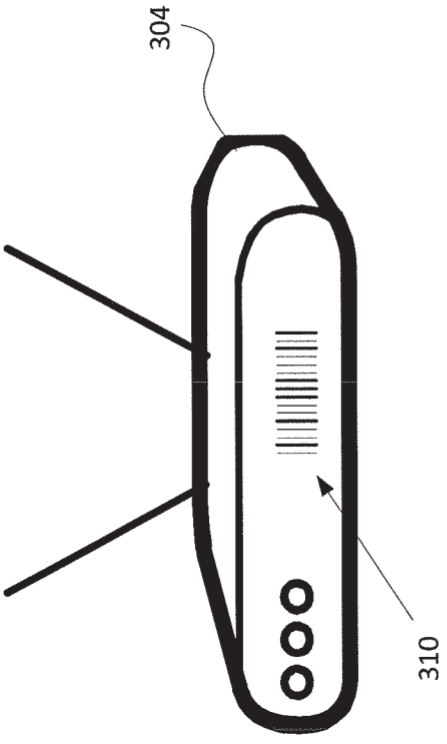

FIG. 3

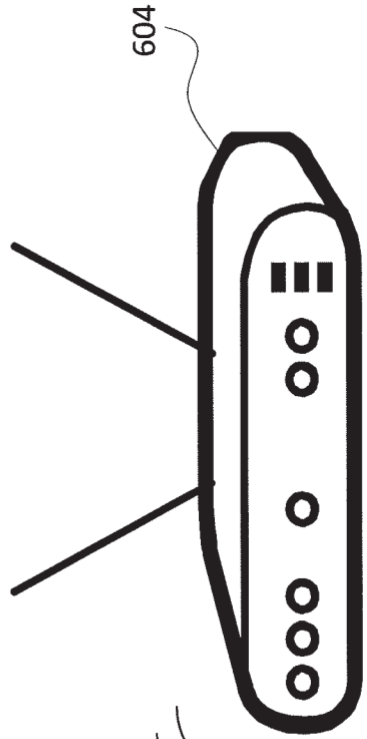

FIG. 6

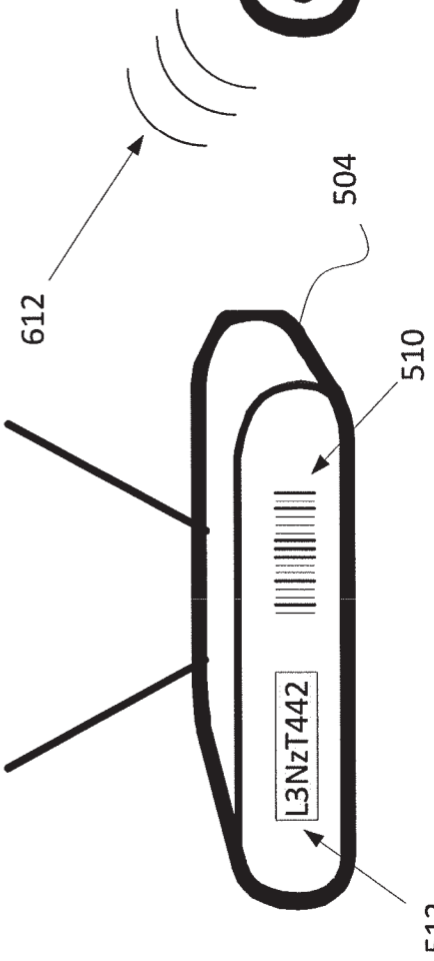

FIG. 5

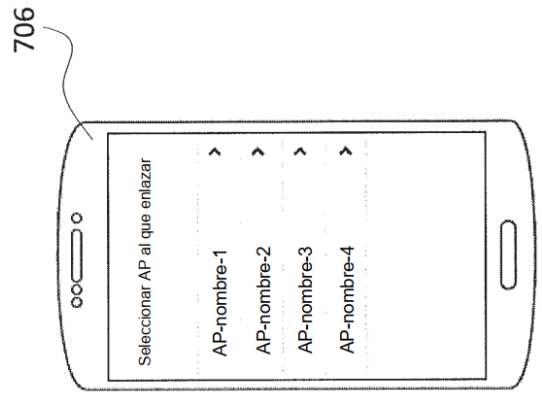

FIG. 7C

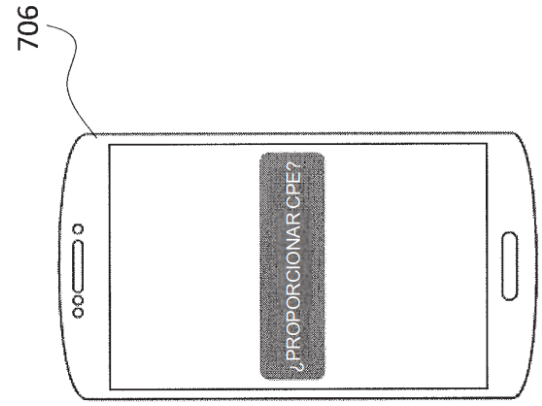

FIG. 7B

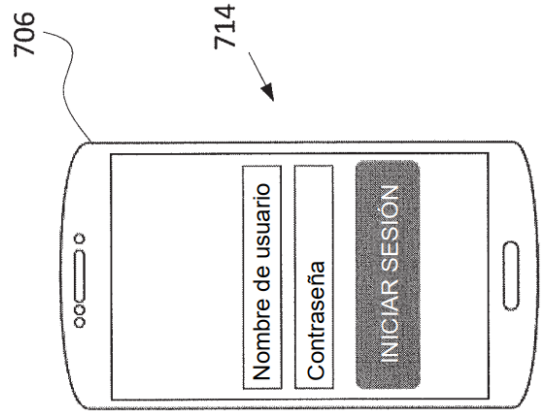

FIG. 7A

FIG. 7D

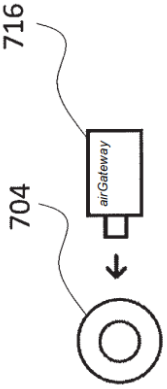

FIG. 7E

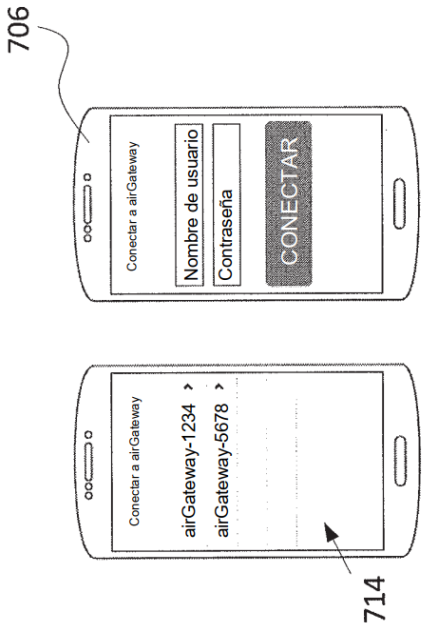

FIG. 7F

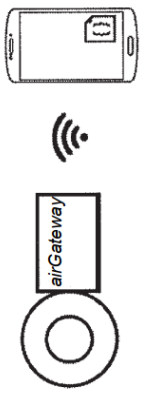

FIG. 7G

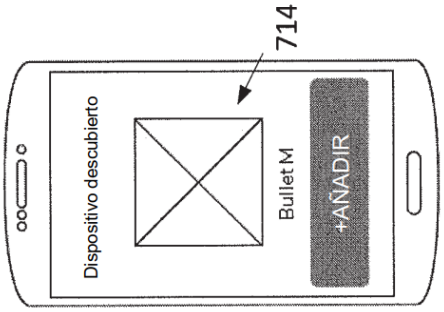

FIG. 7H

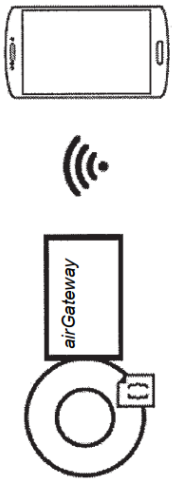

FIG. 7I

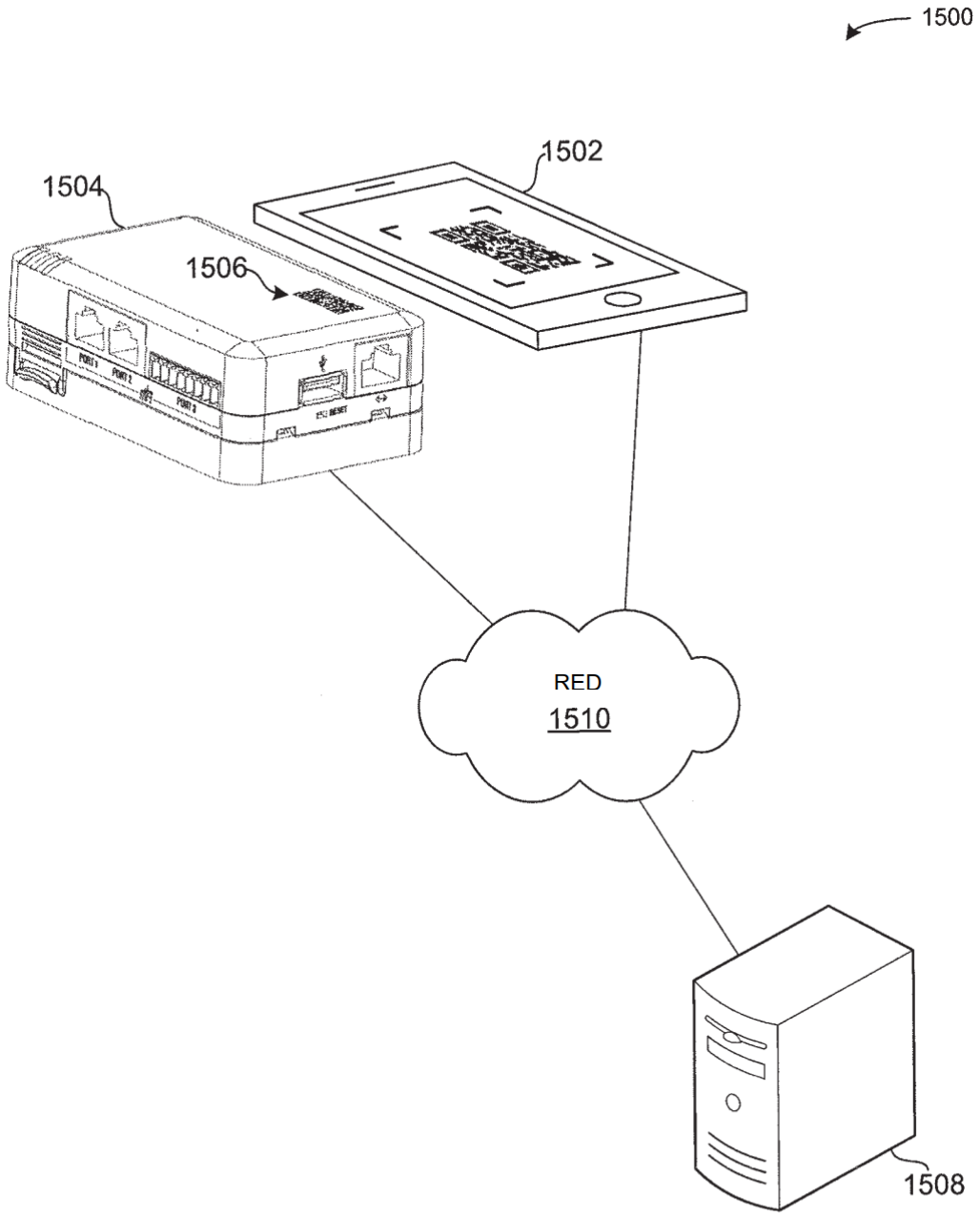

FIG. 8

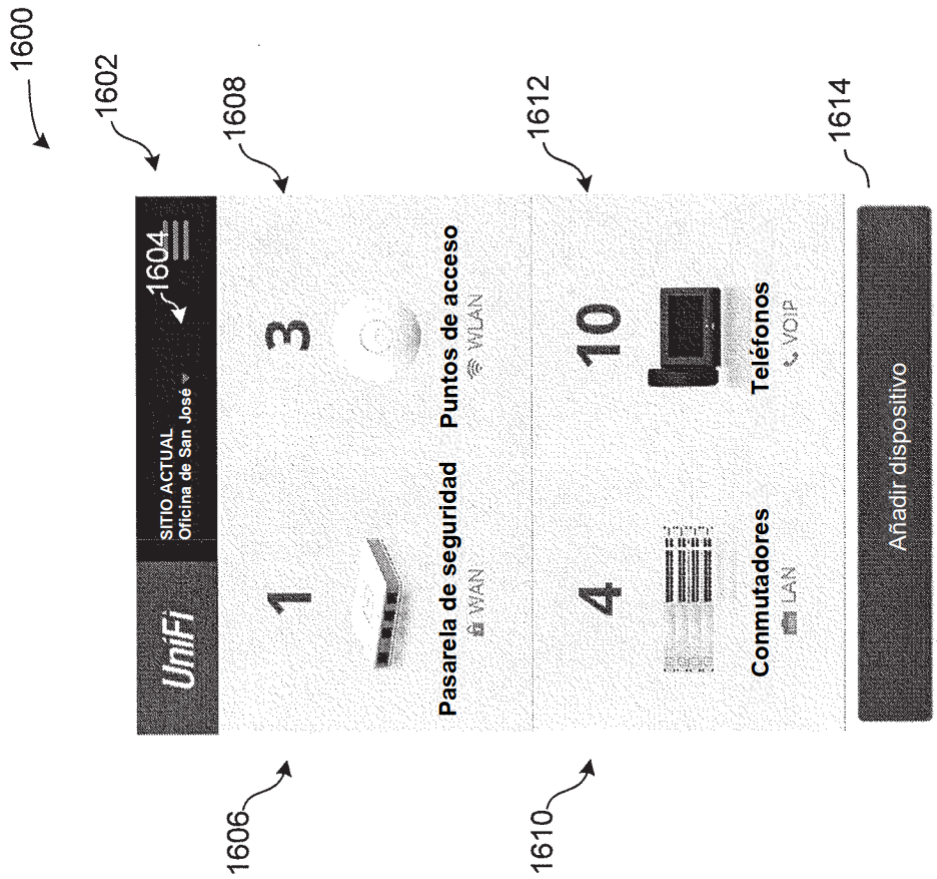
1600
1602
1604
UniFi
SITIO ACTUAL
Oficina de San José
1608
1
3
Pasarela de seguridad
WAN
Puntos de acceso
WLAN
1606
1610
1612
4
10
Conmutadores
LAN
Teléfonos
VOIP
1614
Añadir dispositivo

FIG. 9

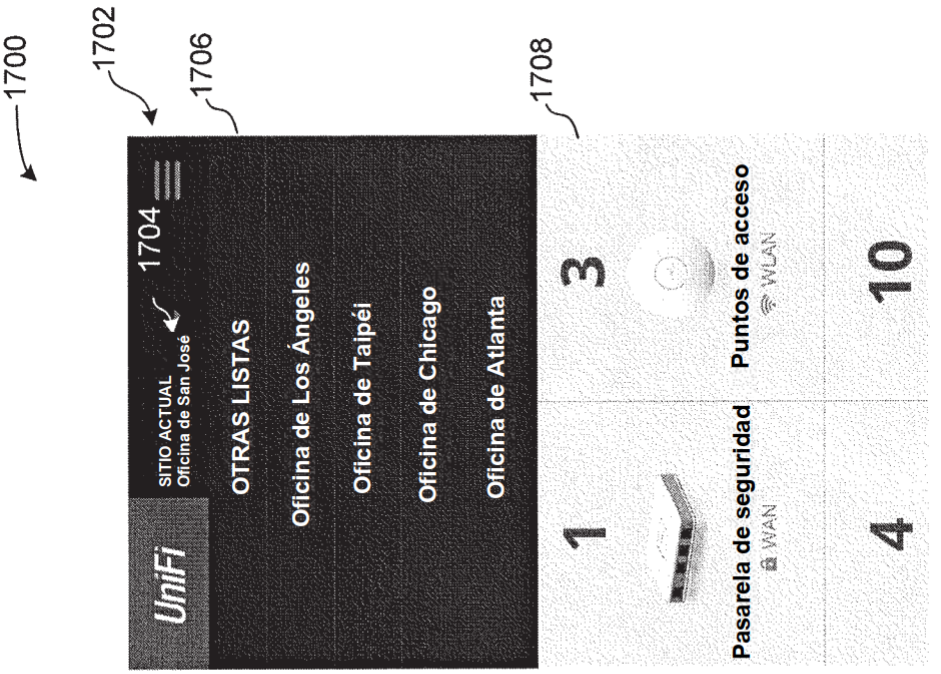
1700
1702
1704
UniFi
SITIO ACTUAL
Oficina de San José
1706
OTRAS LISTAS
Oficina de Los Ángeles
Oficina de Taipéi
Oficina de Chicago
Oficina de Atlanta
1708
1
3
Pasarela de seguridad
WAN
Puntos de acceso
WLAN
4
10

FIG. 10

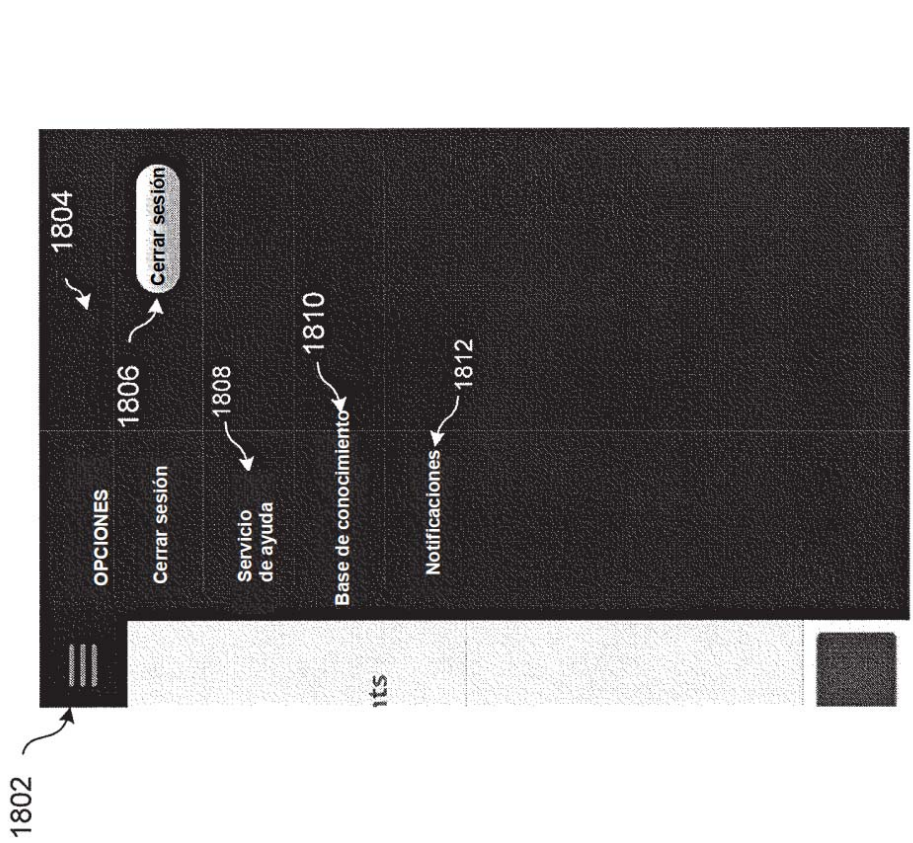
1800
1802
1804
OPCIONES
Cerrar sesión
1806
Cerrar sesión
1808
Servicio de ayuda
1810
Base de conocimiento
1812
Notificaciones
its

FIG. 11

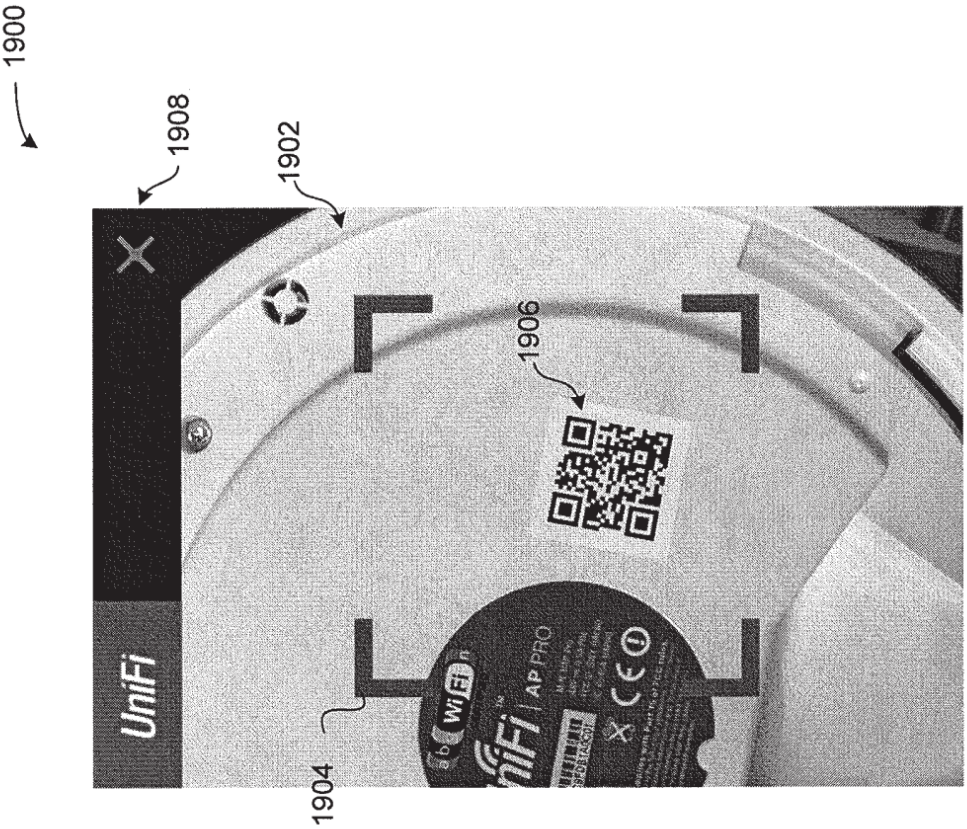
1900
1908
1902
UniFi
1906
1904

FIG. 12

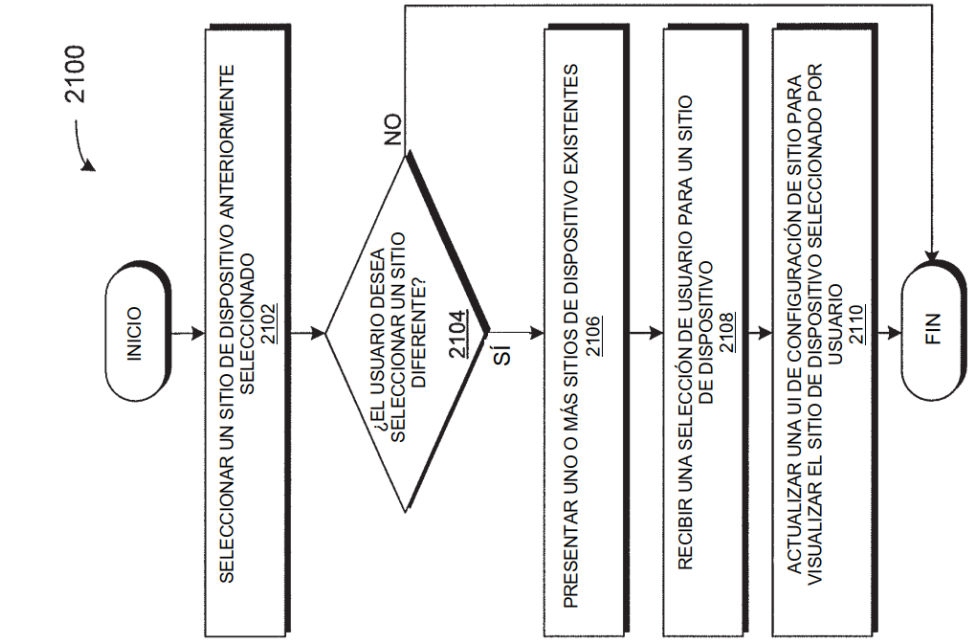
2100
INICIO
SELECCIONAR UN SITIO DE DISPOSITIVO ANTERIORMENTE SELECCIONADO
2102
¿EL USUARIO DESEA SELECCIONAR UN SITIO DIFERENTE?
2104
NO
SÍ
PRESENTAR UNO O MÁS SITIOS DE DISPOSITIVO EXISTENTES
2106
RECIBIR UNA SELECCIÓN DE USUARIO PARA UN SITIO DE DISPOSITIVO
2108
ACTUALIZAR UNA UI DE CONFIGURACIÓN DE SITIO PARA VISUALIZAR EL SITIO DE DISPOSITIVO SELECCIONADO POR USUARIO
2110
FIN

FIG. 14

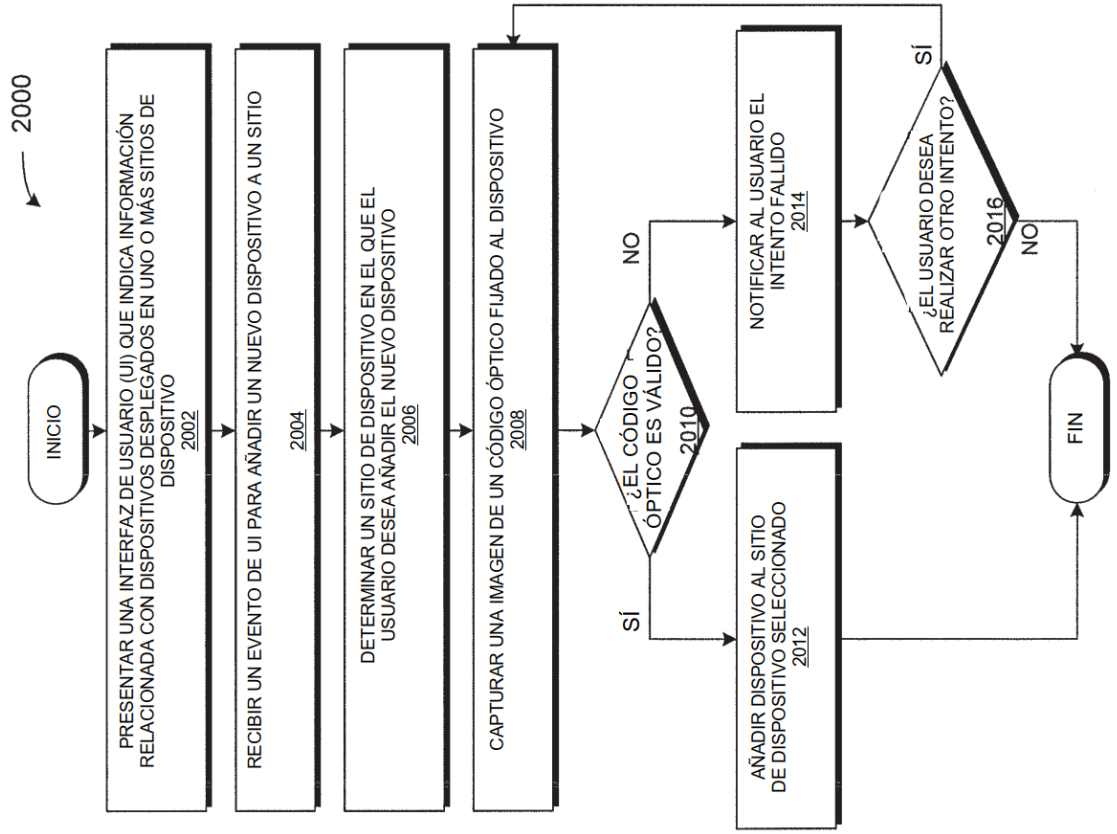
2000
INICIO
PRESENTAR UNA INTERFAZ DE USUARIO (UI) QUE INDICA INFORMACIÓN RELACIONADA CON DISPOSITIVOS DESPLEGADOS EN UNO O MÁS SITIOS DE DISPOSITIVO
2002
RECIBIR UN EVENTO DE UI PARA AÑADIR UN NUEVO DISPOSITIVO A UN SITIO
2004
DETERMINAR UN SITIO DE DISPOSITIVO EN EL QUE EL USUARIO DESEA AÑADIR EL NUEVO DISPOSITIVO
2006
CAPTURAR UNA IMAGEN DE UN CÓDIGO ÓPTICO FIJADO AL DISPOSITIVO
2008
¿EL CÓDIGO ÓPTICO ES VÁLIDO?
2010
NO
SÍ
NOTIFICAR AL USUARIO EL INTENTO FALLIDO
2014
AÑADIR DISPOSITIVO AL SITIO DE DISPOSITIVO SELECCIONADO
2012
¿EL USUARIO DESEA REALIZAR OTRO INTENTO?
2016
SÍ
NO
FIN

FIG. 13

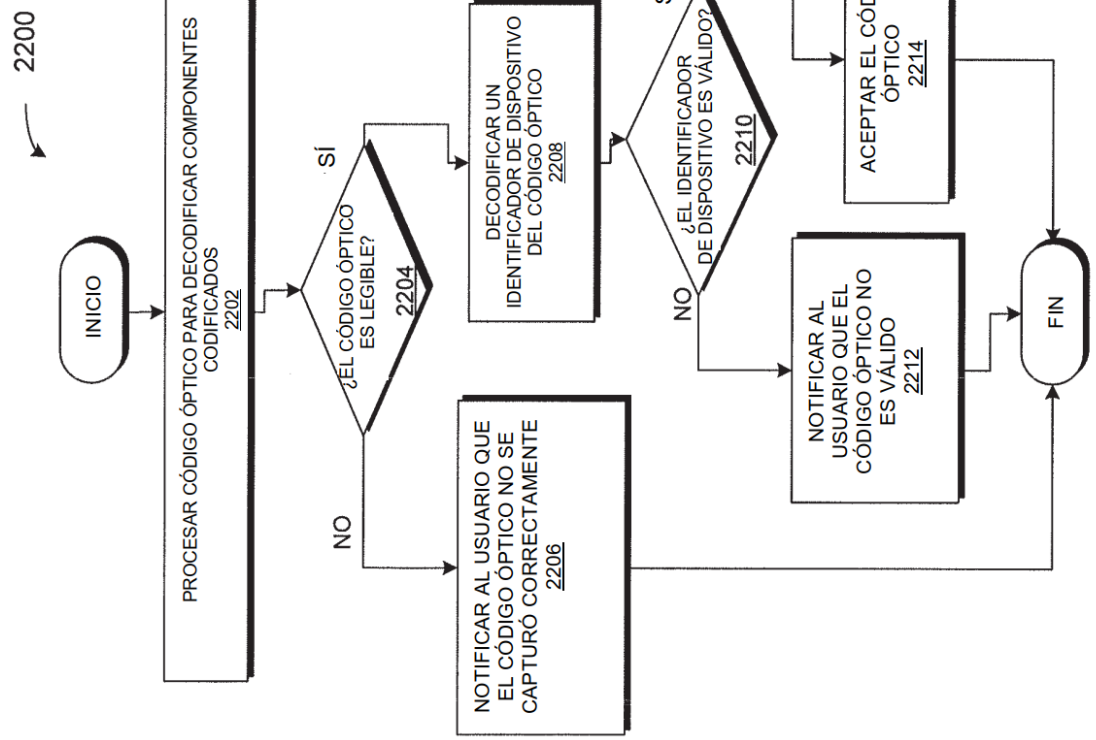
2200
INICIO
PROCESAR CÓDIGO ÓPTICO PARA DECODIFICAR COMPONENTES CODIFICADOS
2202
¿EL CÓDIGO ÓPTICO ES LEGIBLE?
2204
SÍ
NO
NOTIFICAR AL USUARIO QUE EL CÓDIGO ÓPTICO NO SE CAPTURÓ CORRECTAMENTE
2206
DECODIFICAR UN IDENTIFICADOR DE DISPOSITIVO DEL CÓDIGO ÓPTICO
2208
¿EL IDENTIFICADOR DE DISPOSITIVO ES VÁLIDO?
2210
SÍ
NO
ACEPTAR EL CÓDIGO ÓPTICO
2214
NOTIFICAR AL USUARIO QUE EL CÓDIGO ÓPTICO NO ES VÁLIDO
2212
FIN

FIG. 15

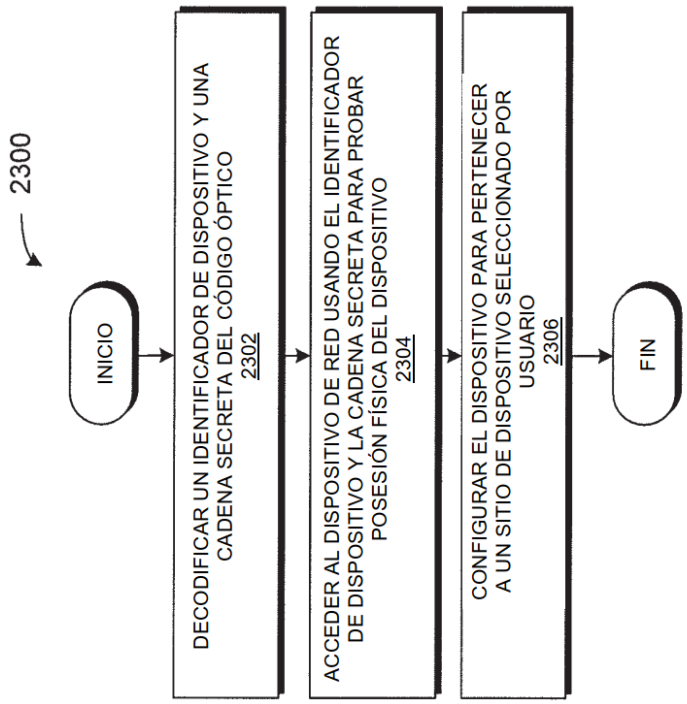
2300
INICIO
DECODIFICAR UN IDENTIFICADOR DE DISPOSITIVO Y UNA CADENA SECRETA DEL CÓDIGO ÓPTICO
2302
ACCEDER AL DISPOSITIVO DE RED USANDO EL IDENTIFICADOR DE DISPOSITIVO Y LA CADENA SECRETA PARA PROBAR POSESIÓN FÍSICA DEL DISPOSITIVO
2304
CONFIGURAR EL DISPOSITIVO PARA PERTENECER A UN SITIO DE DISPOSITIVO SELECCIONADO POR USUARIO
2306
FIN

FIG. 16

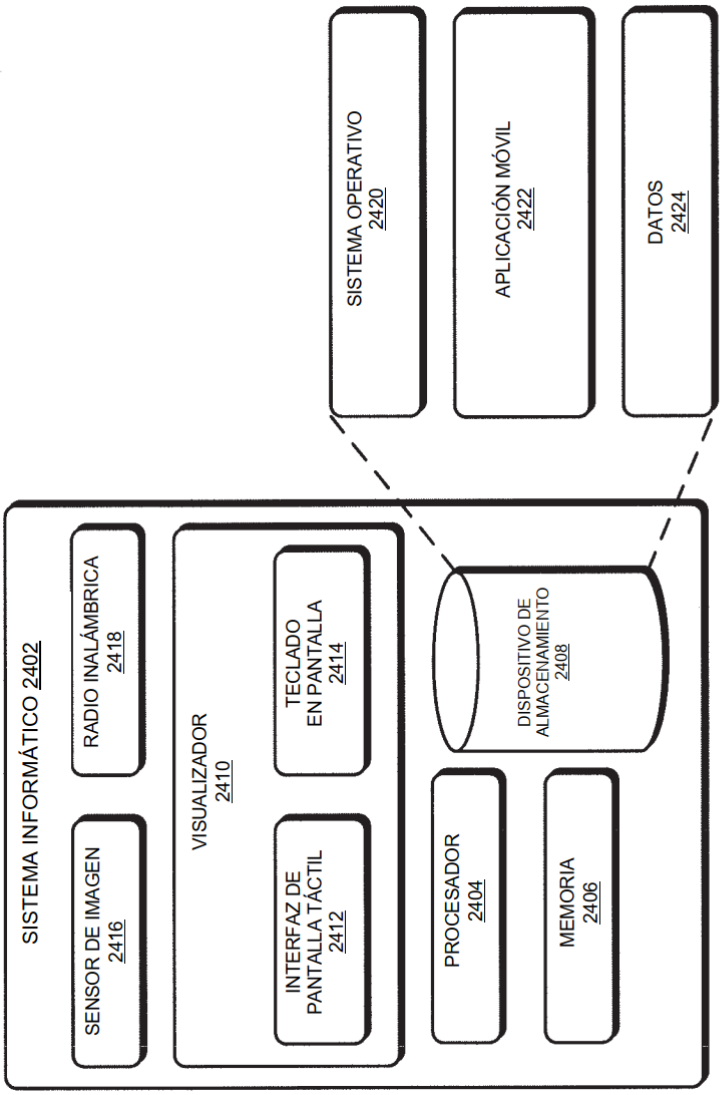
SISTEMA INFORMÁTICO 2402
SENSOR DE IMAGEN 2416
RADIO INALÁMBRICA 2418
VISUALIZADOR 2410
INTERFAZ DE PANTALLA TÁCTIL 2412
TECLADO EN PANTALLA 2414
PROCESADOR 2404
MEMORIA 2406
DISPOSITIVO DE ALMACENAMIENTO 2408
SISTEMA OPERATIVO 2420
APLICACIÓN MÓVIL 2422
DATOS 2424

FIG. 17