(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 523 323**

(51) Int. CI.:

H04W 48/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.09.2008 E 08834360 (3)**

(97) Fecha y número de publicación de la concesión europea: **20.08.2014 EP 2206400**

(54) Título: **Sistemas y métodos para la selección de redes inalámbricas**

(30) Prioridad:

28.09.2007 US 976344 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.11.2014

(73) Titular/es:

DEVICESCAPE SOFTWARE, INC. (100.0%)
1001 BAYHILL DRIVE, SUITE 185
SAN BRUNO, CA 94066, US

(72) Inventor/es:

WYNN, SIMON y
FRASER, DAVID

(74) Agente/Representante:

RIZZO, Sergio

DESCRIPCIÓN

Sistemas y métodos para la selección de redes inalámbricas

ANTECEDENTES

1. Campo de la Invención

[0001] La presente invención se refiere de forma general al acceso a redes de comunicación. Más particularmente, la invención se refiere a la selección de una o varias redes de comunicación inalámbricas.

2. Descripción de la técnica relacionada

[0002] La creciente utilización de las redes para acceder a la información ha dado lugar a una mayor dependencia de la comunicación de red para realizar diversas actividades. Con esta dependencia llega la creciente expectativa de que el acceso a la red será ubicuo. El acceso a la red para usuarios móviles ha aumentado especialmente por las mejoras en la tecnología inalámbrica. Varios móviles (por ejemplo, GSM, CDMA y similares), Wi-Fi (es decir, IEEE 802.11), WiMAX (es decir, IEEE 802.16), y otras tecnologías han permitido un amplio rango de opciones de acceso para un usuario de red potencial. Muchos puntos de acceso inalámbrico o "puntos calientes" sólo son accesibles en regiones geográficas locales, en algunos casos tan pequeñas como un negocio específico u otra dirección. Además, los puntos calientes situados estratégicamente pueden proporcionar acceso a redes públicas o privadas para un grupo diverso de personas.

[0003] Los propietarios o administradores de puntos calientes a menudo requieren una contraseña y similares para permitir el acceso al usuario. Como resultado, un usuario de varios puntos calientes puede tener que almacenar, recordar, o administrar de alguna otra manera un gran número de contraseñas. Muchos usuarios pueden almacenar sus contraseñas en un ordenador portátil que utilicen para acceder al punto caliente. No obstante, no todos los dispositivos capaces de acceder a los puntos calientes son ordenadores portátiles; los teléfonos móviles, los asistentes digitales personales (PDAs) y muchos otros dispositivos son ahora capaces de tener un acceso inalámbrico. Desafortunadamente, los usuarios a menudo no pueden introducir o almacenar fácilmente la contraseña en el dispositivo. Por ejemplo, algunos dispositivos capaces de tener acceso inalámbrico pueden no tener un teclado. Incluso cuando un dispositivo incluye un teclado, el teclado es a menudo pequeño y puede tener una funcionalidad limitada, especialmente para los usuarios con destreza en los dedos limitada.

[0004] Cuando los usuarios almacenan contraseñas en un ordenador portátil, el usuario debe primero acceder al ordenador portátil y almacenar la contraseña correcta en el ordenador. Cuando una contraseña cambia, es necesario que el usuario actualice la contraseña en el ordenador. Además, tener el nombre de usuario y la contraseña almacenados en el dispositivo constituye un problema de seguridad en el caso de que el dispositivo se perdiera o lo robaran.

[0005] Además, normalmente es necesario que los usuarios introduzcan una contraseña, un nombre de usuario y naveguen por un sitio web para obtener acceso a una red. Este proceso requiere tiempo y el usuario puede equivocarse al introducir la información y verse obligado a volver a introducir los datos.

[0006] Cuando los usuarios introducen una contraseña de forma manual, son menos aptos para recordar las contraseñas difíciles. Como resultado, el acceso mediante contraseñas sencillas es susceptible de ser pirateado y puede comprometer el acceso a la red del usuario, el punto caliente y/o la información personal del usuario. Además, se puede robar el acceso a la red del usuario si se piratea o simplemente se adivina la contraseña sencilla del usuario.

[0007] Conectarse a redes inalámbricas ha sido tradicionalmente un proceso complejo para los usuarios de dispositivos inalámbricos por otras razones. Normalmente, el usuario entra en un área en la que están presentes dos o más redes wifi, selecciona la función wifi en su portátil y ve una serie de "resultados de exploración" que listan las redes wifi disponibles. En un ejemplo, el listado de redes wifi disponibles. En un ejemplo, el listado de redes wifi disponibles comprende una lista de identificadores SSID (del inglés *Service Set IDentifier*) de red wifi. El usuario debe identificar a menudo qué red wifi no tiene encriptación u otro mecanismo de seguridad (por ejemplo, una página de acceso). Para aumentar la frustración del usuario, algunas de las redes inalámbricas pueden ser funcionales, mientras que otras pueden estar mal configuradas de tal manera que dejan la red inutilizable.

[0008] El usuario normalmente toma una decisión arbitraria sobre a qué red wifi conectarse basándose en el listado. Al tomar una decisión sobre a qué red wifi conectarse, el usuario normalmente no sabe si la red wifi seleccionada proporcionará una calidad de servicio adecuada o ni siquiera si la red será capaz de proporcionar una dirección IP mediante un "protocolo de configuración dinámica de *host*" (DHCP por sus siglas en inglés).

[0009] US2005/0260973 describe un administrador inalámbrico operable para recibir una solicitud de un dispositivo móvil para comunicar de forma inalámbrica con una red empresarial, incluyendo la solicitud información operable para identificar de forma dinámica una localización del dispositivo móvil.

[0010] US2007/0019670 describe un método y aplicación para seleccionar una red de entre una o varias redes candidatas.

SUMARIO DE LA INVENCIÓN

[0011] La invención se define como un método para seleccionar una red inalámbrica según la reivindicación 1 y como el sistema correspondiente según la reivindicación 7. Según un aspecto de la invención, un método comprende recibir, mediante un servidor procedente de un dispositivo digital, un primer identificador de dispositivo de red para un primer dispositivo de red y un segundo identificador de dispositivo de red para un segundo dispositivo de red, obtener, mediante el servidor, un primer perfil de red que comprende un primer atributo, basándose el primer perfil de red en el primer identificador de dispositivo de red, obtener, mediante el servidor, un segundo perfil de red que comprende un segundo atributo, basándose el segundo perfil de red en el segundo identificador de dispositivo de red, y seleccionar, mediante el servidor, o el primer identificador de dispositivo de red o el segundo identificador de dispositivo de red basándose en un análisis de atributo del primer atributo y del segundo atributo.

[0012] El método puede comprender además proporcionar al dispositivo digital, mediante el servidor, una selección de red inalámbrica o una respuesta a una solicitud de credenciales, basándose en la selección, estando el identificador de selección de red inalámbrica asociado al primer dispositivo de red o al segundo dispositivo de red para permitir al dispositivo digital iniciar un acceso con el primer dispositivo de red asociado o con el segundo dispositivo de red, comprendiendo la respuesta a una solicitud de credenciales las credenciales necesarias para acceder al primer dispositivo de red o al segundo dispositivo de red mediante el dispositivo digital.

[0013] En algunos modos de realización, el identificador de selección de red comprende una lista que incluye el primer identificador de dispositivo de red y el segundo identificador de dispositivo de red ordenados basándose en el análisis de atributo del primer atributo y del segundo atributo. Un atributo puede comprender una medición de rendimiento, un indicador de compartido y un identificador de servicio.

[0014] El método puede comprender además comparar, mediante el servidor, el primer atributo y el segundo atributo con requisitos mínimos, en el que la selección, mediante el servidor, del primer identificador de dispositivo de red o del segundo identificador de dispositivo de red también se basa, al menos en parte, en la comparación de los atributos con los requisitos mínimos. El método puede comprender además comparar, mediante el servidor, el primer atributo y el segundo atributo con una configuración personalizada, en el que la selección, mediante el servidor, del primer identificador de dispositivo de red o del segundo identificador de dispositivo de red también se basa, al menos en parte, en la comparación de los atributos con la configuración personalizada. El método puede comprender además recibir, mediante el servidor, un identificador de usuario y en recuperar la configuración personalizada a partir de una cuenta de usuario basándose en el identificador de usuario.

[0015] Según un aspecto de la invención, un sistema comprende un dispositivo digital y un servidor. El dispositivo digital puede estar conectado a una red de comunicación y configurado para transmitir un primer identificador de dispositivo de red para un primer dispositivo de red y un segundo identificador de dispositivo de red para un segundo dispositivo de red por la red de comunicación. El servidor también puede estar conectado a la red de comunicación y configurado para recibir el primer identificador de dispositivo de red y el segundo identificador de dispositivo de red procedentes del dispositivo digital, para obtener un primer perfil de red que comprende un primer atributo, basándose el primer perfil de red en el primer identificador de dispositivo de red, para obtener un segundo perfil de red que comprende un segundo atributo, basándose el segundo perfil de red en el segundo identificador de dispositivo de red, y para seleccionar o el primer identificador de dispositivo de red o el segundo identificador de dispositivo de red basándose en un análisis de atributo del primer atributo y del segundo atributo.

[0016] Un soporte de almacenamiento legible por ordenador puede configurarse para almacenar un código legible por ordenador con el fin de controlar un ordenador para llevar a cabo el método anteriormente mencionado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0017]

La Figura 1 es un diagrama de un entorno en el que se pueden practicar los modos de realización de la presente invención.

La Figura 2 es un diagrama de bloques de un servidor de credenciales a modo de ejemplo.

La Figura 3 es un diagrama de flujo de un proceso para proporcionar acceso a la red al dispositivo digital a modo de ejemplo.

La Figura 4 es un diagrama de bloques de una solicitud de credenciales a modo de ejemplo.

La Figura 5 es un diagrama de bloques de una respuesta a una solicitud de credenciales a modo de ejemplo.

La Figura 6 es un diagrama de flujo del método para proporcionar credenciales de red a modo de ejemplo.

La Figura 7 es otro diagrama de flujo del método para proporcionar credenciales de red a modo de ejemplo.

La Figura 8 es un diagrama de flujo de un método para recibir y almacenar credenciales de red a modo de ejemplo.

La figura 9 es un diagrama de bloques de un servidor de credenciales a modo de ejemplo.

La Figura 10 es un diagrama de otro entorno en el que se pueden practicar los modos de realización de la presente invención.

La Figura 11 es un diagrama de flujo de un proceso para proporcionar una selección de una red inalámbrica a modo de ejemplo.

La Figura 12 es un diagrama de flujo de un proceso para seleccionar una red inalámbrica a modo de ejemplo.

La Figura 13 es un diagrama para seleccionar una red inalámbrica y acceder a la red inalámbrica seleccionada.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

[0018] Los modos de realización de la presente invención ofrecen sistemas y métodos para proporcionar credenciales de red. En modos de realización de ejemplo, un servidor de credenciales recibe una solicitud de credenciales de red procedente de un dispositivo digital en un punto caliente. A la solicitud se le puede dar formato como un protocolo estándar que se transmite desde el punto caliente hasta el servidor de credenciales. El servidor de credenciales puede identificar un registro de red basándose en al menos parte de información contenida en la solicitud y transmitir al dispositivo digital las credenciales de red asociadas al registro de red. El dispositivo digital puede recibir las credenciales de red y proporcionárselas al dispositivo de red para obtener acceso a la red.

[0019] En varios modos de realización, un servidor de normas puede identificar una red preferida a partir de una multitud de redes disponibles a la que el dispositivo digital puede conectar basándose en una variedad de atributos de red. En un ejemplo, un dispositivo digital puede examinar una región física en busca de redes disponibles y generar una lista de redes inalámbricas disponibles. La lista se puede proporcionar a un servidor de normas que identifica y recupera un perfil de red para cada red inalámbrica de la lista. El servidor de normas puede entonces comparar cada perfil de red (por ejemplo, mediante los atributos contenidos en cada perfil) para seleccionar una red preferida de la lista. El servidor de normas puede transmitir entonces la selección de red inalámbrica al dispositivo digital que puede entonces acceder a la red.

[0020] En algunos modos de realización, el dispositivo digital accede a la red inalámbrica seleccionada utilizando credenciales proporcionadas por el servidor de credenciales. En un ejemplo, cuando el servidor de normas selecciona la red inalámbrica preferida, el servidor de normas (u otro servidor en comunicación con el servidor de normas) puede proporcionar simultáneamente (o casi simultáneamente) una respuesta a una solicitud de credenciales incluyendo credenciales de red asociadas a la red inalámbrica seleccionada.

[0021] La Figura 1 ilustra un diagrama de un entorno 100 en el que se pueden practicar los modos de realización de la presente invención. En modos de realización de ejemplo, un usuario con un dispositivo digital 102 entra en un punto caliente. El dispositivo digital 102 puede transmitir automáticamente una solicitud de credenciales como un protocolo estándar por un dispositivo de red 104. La solicitud de credenciales se puede reenviar a un servidor de credenciales 116 que, basándose en la información contenida en la solicitud de credenciales, transmite una respuesta a una solicitud de credenciales de vuelta al dispositivo digital 102. La respuesta a la solicitud de credenciales contiene credenciales de red que el dispositivo digital 102 puede proporcionar al dispositivo de red 104, al servidor de autenticación 108, o al controlador de acceso 112 para obtener acceso a la red de comunicación 114.

[0022] En varios modos de realización, un punto caliente comprende el dispositivo de red 104, el servidor de autenticación 108, el servidor DNS 110 y el controlador de acceso 112 que están conectados a la red de área local 106 (por ejemplo, un "jardín vallado"). El dispositivo de red 104 puede comprender un punto de acceso que permite al dispositivo digital 102 comunicar con el servidor de autenticación 108, el servidor DNS 110 y el controlador de acceso 112 por la red de área local 106. El dispositivo digital 102 puede comprender un portátil, un teléfono móvil, una cámara, un asistente digital personal, o cualquier otro dispositivo informático. El servidor de autenticación 108 es un servidor que requiere credenciales de red del dispositivo digital 102 antes de permitir al dispositivo digital 102 acceder a la red de comunicación 114. EL servidor DNS 110 proporciona servicios DNS por la red de área local 106 y puede transmitir solicitudes a otros servidores DNS (no se muestra) a través de la red de comunicación 114. El controlador de acceso 112 es un dispositivo de acceso como un *router* o puente de red que puede permitir la comunicación entres dispositivos comunicados operativamente al dispositivo de red 104 y dispositivos conectados a la red de comunicación 114.

[0023] Aunque el punto caliente de la Figura 1 representa servidores separados conectados a la red de área local 106, los expertos en la materia entenderán que puede haber cualquier número de dispositivos (por ejemplo, servidores, dispositivos digitales, controladores de acceso y dispositivos de red) conectados a la red de área local 106. En algunos modos de realización, la red de área local 106 es opcional. En un ejemplo, el servidor de autenticación 108, el servidor DNS 110, y el controlador de acceso 112 están conectados directamente al dispositivo de red 104. En varios modos de realización, el servidor de autenticación 108, el servidor DNS 110 y el controlador de acceso 112 pueden combinarse en uno o varios servidores o en uno o varios dispositivos digitales. Además, aunque la Figura 1 representa acceso inalámbrico, el dispositivo digital 102 se puede conectar al dispositivo de red 104 de manera inalámbrica o por cables (por ejemplo, en 10baseT).

[0024] Para acceder a la red de comunicación 114, el servidor de autenticación 108 puede necesitar que el dispositivo digital 102 proporcione una o varias credenciales de red para acceder al punto caliente. La credencial de red puede comprender, por ejemplo, un nombre de usuario y una contraseña para una cuenta asociada al punto caliente. En modos de realización alternativos, se pueden utilizar credenciales de red distintas a un nombre de usuario y una contraseña.

[0025] Según modos de realización de ejemplo, el dispositivo digital 102 puede adquirir dinámicamente las credenciales de red del servidor de credenciales 116. El dispositivo digital 102 puede enviar al servidor de credenciales 116 una solicitud de credenciales que comprende una identidad del dispositivo digital 102 (o del usuario del dispositivo digital 102) y detalles sobre el dispositivo de red 104 (por ejemplo, el nombre del dispositivo de red 104 o el del proveedor del servicio wifi).

[0026] En un ejemplo, cuando el dispositivo digital 102 entra en el punto caliente, el dispositivo de red 104 puede proporcionar una dirección IP a la que se pueden enviar consultas de DNS, por ejemplo, mediante un protocolo de configuración dinámica de *host*. La solicitud de credenciales puede tener el formato de un protocolo estándar. En un ejemplo, la solicitud de credenciales puede tener el formato de una solicitud DNS. La solicitud de credenciales puede ser una solicitud de registro de texto (por ejemplo, TXT), que comprende un tipo de registro estándar de manera que la infraestructura de red (por ejemplo, el controlador de acceso 112) no bloquee la solicitud.

[0027] En algunos modos de realización, la solicitud de credenciales es recibida por el servidor DNS 110, el cual puede remitir la solicitud de credenciales al servidor de credenciales 116 para la credencial de red. En modos de realización de ejemplo, el servidor de credenciales 116 puede realizar una búsqueda para determinar la(s) credencial(es) de red apropiada(s) para enviarlas de vuelta al servidor DNS 110, que remite la credencial de red de vuelta al dispositivo digital solicitante 102. En varios modos de realización, la(s) credencial(es) de red apropiada(s) se envían desde el servidor de credenciales 116 hasta el dispositivo digital 102 por la misma ruta que la transmisión de la solicitud de credenciales.

[0028] Aunque sólo se representa un servidor DNS 110 en la Figura 1, la solicitud de credenciales se puede remitir a cualquier número de servidores, incluyendo, pero sin carácter limitativo, servidores DNS, antes de que la reciba el servidor de credenciales 116. En otros modos de realización, la solicitud de credenciales se remite directamente desde el dispositivo de red 104 hasta el servidor de credenciales 116.

[0029] En algunos modos de realización, una respuesta a una solicitud de credenciales procedente del servidor de credenciales 116 puede comprender el nombre de usuario, la contraseña y/o información del procedimiento de acceso. La información del procedimiento de acceso puede comprender, por ejemplo, nombres de elementos en formato HTML, un URL de envío o un protocolo de envío. En algunos modos de realización, el servidor de credenciales 116 puede encriptar la respuesta de credencial de red utilizando una clave de encriptación asociada al dispositivo digital 102 antes de transmitirla de vuelta al dispositivo digital 102.

[0030] Una vez que el dispositivo digital 102 recibe la respuesta de credencial de red, el dispositivo digital 102 puede enviar la credencial de red (recuperada de la respuesta de credencial de red) al dispositivo de red 104 en una respuesta de autenticación. En modos de realización de ejemplo, la respuesta de autenticación se puede

remitir a un servidor de autenticación 108 para verificarla. En algunos modos de realización, el servidor de autenticación 108 puede comprender un servidor AAA o un servidor RADIUS.

[0031] Cabe señalar que la Figura 1 es a modo de ejemplo. Modos de realización alternativos pueden comprender más componentes, menos componentes o componentes funcionalmente equivalentes y aún así estar dentro del alcance de los presentes modos de realización. Por ejemplo, como se ha mencionado anteriormente, las funciones de los diversos servidores (por ejemplo, servidor DNS 110, servidor de credenciales 116 y servidor de autenticación 108) se pueden combinar en uno o dos servidores. Es decir, por ejemplo, el servidor de autenticación 108 y el servidor DNS 110 pueden comprender el mismo servidor, o la funcionalidad del servidor de autenticación 108, el servidor DNS 110 y el controlador de acceso 112 pueden combinarse en un solo dispositivo.

[0032] La Figura 2 es un diagrama de bloques de un servidor de credenciales 116 a modo de ejemplo. El servidor de credenciales 116 comprende un módulo de autenticación 200, un módulo de red 202, un módulo de solicitud de credenciales 204, un módulo de respuesta a la solicitud de credenciales 206, un módulo de encriptación/desencriptación 208, un almacenamiento de registros de red 210 y un almacenamiento de claves de encriptación 212. Un módulo puede comprender, de forma individual o combinada, *software*, *hardware*, *firmware* o un sistema de circuitos.

[0033] El módulo de autenticación 200 puede configurarse para autenticar la solicitud de credenciales y proporcionar seguridad a la respuesta a la solicitud de credenciales. En varios modos de realización, el dispositivo digital 102 puede encriptar o firmar digitalmente la solicitud de credenciales utilizando una clave de encriptación (por ejemplo, una clave de encriptación compartida o una clave de encriptación que es una parte de un par de claves). El módulo de autenticación 200 puede autenticar la solicitud de credenciales desencriptando la solicitud de credenciales con la clave de encriptación adecuada recuperada del almacenamiento de claves de encriptación 212. En un ejemplo, el dispositivo digital 102 genera un resumen criptográfico (*hash*) de la solicitud de credenciales y almacena el resumen criptográfico en una parte encriptada de la solicitud de credenciales. El módulo de autenticación 200 puede desencriptar la solicitud de credenciales, generar un resumen criptográfico de la respuesta a la solicitud de credenciales y comparar el resumen criptográfico generado con el resumen criptográfico contenido en la solicitud de credenciales para autenticarlo.

[0034] En otros modos de realización, el dispositivo digital 102 puede generar un número aleatorio utilizado sólo una vez (*nonce*) (es decir, un valor aleatorio) y almacenarlo en una parte de la solicitud de credenciales que está firmada digitalmente. El módulo de autenticación 200 puede desencriptar la firma digital para autenticar la solicitud de credenciales y recuperar el *nonce*. En varios modos de realización, cuando el módulo de respuesta a la solicitud de credenciales 206 genera la respuesta a la solicitud de credenciales (que se describe más adelante en el texto), el módulo de autenticación 200 puede incluir el *nonce* en la respuesta a la solicitud de credenciales. El módulo de autenticación 200 o el módulo de encriptación/desencriptación 208 puede entonces encriptar la respuesta a la solicitud de credenciales. Cuando el dispositivo digital 102 desencripta la respuesta a la solicitud de credenciales, el dispositivo digital 102 puede recuperar el *nonce* a partir de la respuesta a la solicitud de credenciales y compararlo con el *nonce* que se transmitió en la solicitud de credenciales para autenticación adicional.

[0035] El módulo de red 202 se puede configurar para recibir la solicitud de credenciales y transmitir la respuesta a la solicitud de credenciales por la red de comunicación 114.

[0036] El módulo de solicitud de credenciales 204 puede recibir del módulo de red 202 la solicitud de credenciales. La solicitud de credenciales puede ser un protocolo estándar. En un ejemplo, la solicitud de credenciales es un protocolo UDP (del inglés *User Datagram Protocol*) (por ejemplo, DNS).

[0037] En modos de realización de ejemplo, el módulo de solicitud de credenciales 204 puede recuperar de la solicitud de credenciales el DDID (del inglés *Digital Data Interface Device*) y el SSID. El DDID puede identificar el dispositivo digital 102, el usuario del dispositivo digital 102 y/o el usuario asociado al registro de red. EL SSID puede identificar el punto caliente o el proveedor de servicios (es decir, el operador) del punto caliente.

[0038] El módulo de solicitud de credenciales 204 o el módulo de respuesta a la solicitud de credenciales 206 pueden identificar un registro de red basándose en el DDID y en el SSID. Un registro de red es un registro asociado [ya sea directa o indirectamente (por ejemplo, una base de datos relacional)] al DDID y al SSID. En un ejemplo, un registro de red contiene las credenciales de red necesarias para proporcionar acceso a la red a un dispositivo digital 102 asociado al DDID en el punto caliente asociado al SSID. Los registros de red se pueden almacenar en el almacenamiento de registros de red 210.

[0039] El módulo de respuesta a la solicitud de credenciales 206 puede generar la respuesta a la solicitud de credenciales. En varios modos de realización, el módulo de respuesta a la solicitud de credenciales 206 recibe del registro de red la credencial de red asociada al DDID y al SSID. En algunos modos de realización, la credencial de red puede comprender un número de tarjeta de crédito. En un ejemplo, el dispositivo digital 102 recibe la credencial de red, recupera el número de tarjeta de crédito y se lo proporciona al servidor de

autenticación 108. En algunos ejemplos, el servidor de autenticación 108 puede entonces cargar una tasa en una tarjeta de crédito asociada al número de tarjeta de crédito o utilizar la información para confirmar la identidad del usuario antes de conceder el acceso a la red.

[0040] Además, en varios modos de realización, las credenciales de red pueden comprender información del procedimiento de acceso. En un ejemplo, la credencial incluye un nombre de usuario y una contraseña que se han de proporcionar en un formulario (por ejemplo, un formulario de autenticación) que el dispositivo digital 102 recupera del servidor de autenticación 108. En algunos modos de realización, la información del procedimiento de acceso puede mandar al dispositivo digital 102 que rellene campos específicos en el formulario con las credenciales de red antes de enviar el formulario completo al servidor de autenticación 108. Los expertos en la materia entenderán que hay muchas maneras de proporcionar credenciales al servidor de autenticación 108.

[0041] El módulo de respuesta a la solicitud de credenciales 206 o el módulo de encriptación/desencriptación 208 pueden encriptar la respuesta a la solicitud de credenciales con una clave de encriptación asociada al DDID o a la solicitud de credenciales. En un ejemplo, el servidor de credenciales 116 almacena una o varias claves de encriptación compartidas. Cada clave de encriptación compartida puede ser compartida por al menos un dispositivo digital 102. El módulo de respuesta a la solicitud de credenciales 206 puede encriptar la respuesta a la solicitud de credenciales con la clave de encriptación compartida asociada al dispositivo digital 102 (por ejemplo, la clave de encriptación compartida se puede asociar al DDID). El módulo de respuesta a la solicitud de credenciales 206 o el módulo de encriptación/desencriptación 208 también pueden encriptar la solicitud de credenciales con una clave de encriptación que es parte de un par de claves. El módulo de encriptación/desencriptación 208 puede encriptar la solicitud de credenciales de muchas maneras.

[0042] El módulo de encriptación/desencriptación 208 puede desencriptar la solicitud de credenciales y encriptar la respuesta a la solicitud de credenciales. Como se ha mencionado anteriormente, el módulo de encriptación/desencriptación 208 puede desencriptar la firma digital de la solicitud de credenciales. En un ejemplo, el módulo de encriptación/desencriptación 208 desencripta la firma digital basándose en una clave de encriptación que está asociada al DDID contenido en la solicitud de credenciales. El módulo de encriptación/desencriptación 208 puede también encriptar la respuesta a la solicitud de credenciales. En un ejemplo, el módulo de encriptación/desencriptación 208 encripta la respuesta a la solicitud de credenciales basándose en una clave de encriptación asociada al DDID (por ejemplo, una clave de encriptación compartida o una clave de encriptación que es parte de un par de claves).

[0043] En varios modos de realización, el módulo de encriptación/desencriptación 208 puede encriptar los registros de red contenidos en el almacenamiento de registros de red 210 y gestionar el almacenamiento de claves de encriptación 212. El módulo de encriptación/desencriptación 208 también puede establecer comunicaciones seguras [por ejemplo, mediante el protocolo de capa de conexión segura (llamado también SSL, por sus siglas en inglés *Secure Sockets Layer*) y el protocolo HTTPS] con un dispositivo digital cuando almacena las credenciales de red. Este proceso se describe con más detalle en la Figura 7. Según algunos modos de realización, el módulo de encriptación/desencriptación 208 puede ser opcional.

[0044] El almacenamiento de registros de red 210 y el almacenamiento de claves de encriptación 212 pueden almacenar registros de red y claves de encriptación, respectivamente. El almacenamiento de registros de red 210 y el almacenamiento de claves de encriptación 212 pueden comprender una o varias bases de datos. En un ejemplo, el almacenamiento de registros de red 210 puede almacenar registros de red. Un registro de red puede comprender un DDID, un SSID y credenciales de red. El registro de red también puede comprender un nombre de usuario y una contraseña para que el usuario acceda, altere, actualice o almacene registros de red en el servidor de credenciales 116.

[0045] En varios modos de realización, el registro de red también puede permitir a varios dispositivos digitales 102 utilizar las mismas credenciales de red. En un ejemplo, el usuario puede poseer varios dispositivos digitales 102. Varios DDIDs, cada DDID asociado a un dispositivo digital diferente 102, pueden incluirse en el mismo registro de red. En algunos modos de realización, varios dispositivos pueden estar asociados a uno o varios registros de red y tales uno o varios registros de red están asociados a un usuario. Como resultado, el usuario puede recuperar las credenciales de red para un punto caliente utilizando cualquier número de dispositivos digitales 102. Los expertos en la materia entenderán que hay muchas maneras de almacenar y organizar los registros de red y/o la información contenida en los mismos (por ejemplo, diferentes estructuras de datos, bases de datos, registros, esquemas de organización, y/o metodologías).

[0046] La Figura 3 es un diagrama de flujo de un proceso para proporcionar acceso a la red al dispositivo digital 102 a modo de ejemplo. Cuando el dispositivo digital 102 entra por primera vez en un punto caliente, el dispositivo digital 102 puede examinar la red de área local 106 en la etapa 300. Como resultado del examen, el dispositivo de red 104 puede proporcionar información de configuración de red en la etapa 302. La información de configuración de red puede comprender una o varias direcciones IP para acceder al servidor DNS 110.

[0047] En la etapa 304, el dispositivo digital 102 genera una solicitud de credenciales. Posteriormente, la solicitud de credenciales se puede enviar al servidor DNS 110 en la etapa 306 utilizando una de las direcciones IP previamente recibidas del dispositivo de red 104.

[0048] Basándose en la solicitud de credenciales, el servidor DNS 110 identifica el servidor de credenciales 116 es en la etapa 308. En otros modos de realización, el servidor DNS 110 remite la solicitud de credenciales al servidor de credenciales 116. Cuando el servidor DNS 110 no es capaz de resolver localmente la solicitud DNS, la solicitud de credenciales se remite a otro servidor DNS en la red de comunicación 114 (por ejemplo, por el puerto 53) que puede entonces remitir la solicitud de credenciales al servidor de credenciales 116. La solicitud de credenciales se remite, ya sea directa o indirectamente a través de uno o varios servidores DNS en la red de comunicación 114, al servidor de credenciales 116 en la etapa 310.

[0049] El servidor de credenciales 116 identifica la credencial de red necesaria basándose en la solicitud de credenciales en la etapa 312. Por ejemplo, la solicitud de credenciales puede comprender un identificador (es decir, el DDID) para el dispositivo digital 102 así como un identificador para el SSID del punto caliente (por ejemplo, el proveedor de servicios tal como un operador). Los identificadores pueden compararse con una tabla (por ejemplo, un registro de red) de tales identificadores mediante el módulo de solicitud de credenciales 204 o el módulo de respuesta a la solicitud de credenciales 206 para determinar la credencial de red apropiada. El módulo de respuesta a la solicitud de credenciales 206 genera entonces una respuesta a la solicitud de credenciales en la etapa 314 y se transmite de vuelta al servidor DNS 110 en la etapa 316. El servidor DNS 110 remite la respuesta a la solicitud de credenciales de vuelta al dispositivo digital en la etapa 318.

[0050] El dispositivo digital 102 puede entonces recuperar las credenciales de red a partir de la respuesta a la solicitud de credenciales en la etapa 320. La credencial de red se le puede proporcionar entonces al dispositivo de red 104 en la etapa 322. Tras verificar las credenciales de red, el dispositivo de red 104 proporciona acceso a la red al dispositivo digital 102 en la etapa 324.

[0051] Haciendo referencia ahora a la Figura 4, se muestra con más detalle una solicitud de credenciales 400 a modo de ejemplo. Según modos de realización de ejemplo, el módulo de solicitud de credenciales 204 puede generar la solicitud de credenciales 400. En un modo de realización, la solicitud de credenciales 400 puede ser una cadena de DNS con una estructura que comprende un identificador de localización 402, un identificador de secuencia 404, un firma 406, el DDID 408, un identificador de conjunto de servicios (SSID) 410 y un identificador de versión 412.

[0052] El identificador de localización 402 opcional puede indicar una localización física o geográfica del dispositivo digital 102, del dispositivo de red 104, del servidor de autenticación 108 o del controlador de acceso 112. En varios modos de realización, el servidor de credenciales 116 puede utilizar el identificador de localización 402 para rastrear la utilización de puntos calientes, los usuarios del dispositivo digital 102, así como el dispositivo digital 102.

[0053] El identificador de secuencia 404 puede comprender cualquier número o conjunto de números utilizados para corresponder a una solicitud posterior al servidor de credenciales 116 para determinar si el acceso se realiza correctamente. Es decir, el identificador de secuencia 404 proporciona un mecanismo de correlación mediante el cual el servidor de credenciales 116 puede realizar la verificación del proceso de acceso.

[0054] En modos de realización alternativos, la firma 406 comprende una firma criptográfica (es decir, una firma digital) que se utiliza para evitar la suplantación. El servidor de credenciales 116 verifica la firma 406 de la solicitud del dispositivo digital 102. Si la firma 406 no es válida, entonces el servidor de credenciales 116 rechaza la solicitud.

[0055] El DDID 408 comprende un identificador del dispositivo digital 102. Por ejemplo, el DDID 408 puede comprender una dirección MAC o cualquier otro identificador del dispositivo digital 102.

[0056] El SSID 410 comprende un identificador del punto de acceso a la red o del proveedor de servicio wifi. Por ejemplo, el SSID 410 puede comprender el nombre del proveedor de servicios o el nombre de la ubicación en la que opera el dispositivo de red 104.

[0057] El identificador de versión 412 puede identificar el protocolo o el formato de la solicitud de credenciales 400. Por ejemplo, un dispositivo digital 102 puede generar la solicitud de credenciales 400 y organizar los datos en un número de formatos diferentes. Cada formato diferente se puede asociar a un identificador de versión diferente. En algunos modos de realización, los componentes del módulo de respuesta a la solicitud de credenciales 206 se pueden actualizar, reconfigurar o alterar con el tiempo, lo que puede afectar a la estructura de la solicitud de credenciales 400. Como resultado, el servidor de credenciales 116 puede recibir una multitud de solicitudes de credenciales 400 que tienen formatos diferentes. El servidor de credenciales 116 puede acceder a la información requerida de cada solicitud de credenciales basándose en el identificador de versión correspondiente.

[0058] La Figura 5 es un diagrama de bloques de una respuesta a una solicitud de credenciales a modo de ejemplo. Según modos de realización de ejemplo, el módulo de respuesta a la solicitud de credenciales 206 puede generar la respuesta a la solicitud de credenciales 500. En un modo de realización, la respuesta a la solicitud de credenciales 500 puede comprender texto encriptado 502. El texto encriptado puede comprender un *nonce* opcional 504 e información de credenciales 506. La información de credenciales puede comprender pares de claves/valores 508 hasta 510.

[0059] Como se ha mencionado anteriormente, la respuesta a la solicitud de credenciales puede tener el formato de una respuesta DNS que comprende texto encriptado 502. El texto encriptado 502 incluye las credenciales de red (por ejemplo, nombre de usuario, contraseña e información del procedimiento de acceso). Aunque la respuesta a la solicitud de credenciales 500 se representa como si incluyera texto encriptado 502, el texto de la respuesta a la solicitud de credenciales 500 no necesita estar encriptado.

[0060] El texto encriptado 502 puede comprender el *nonce*. El *nonce*, como se ha mencionado anteriormente, se puede recuperar de la solicitud de credenciales. Una vez que el dispositivo digital 102 recibe la respuesta a la solicitud de credenciales 500, el dispositivo digital 102 puede comparar el *nonce* en la respuesta a la solicitud de credenciales 500 con el *nonce* transmitido en la solicitud de credenciales para autenticación. Aunque en la Figura 5 el *nonce* se representa como si estuviera en la respuesta a la solicitud de credenciales 500, el *nonce* es opcional.

[0061] La información de credenciales 506 puede comprender un nombre de usuario, una contraseña, información del procedimiento de acceso o una combinación de los mismos. La información de credenciales 506 puede comprender pares de claves/valores 508 hasta 510. Puede haber cualquier número de pares de claves/valores en la información de credenciales 506. Los pares de claves/valores pueden representar la información de credenciales que el dispositivo digital 102 ha de recibir y traducir. La información de credenciales 506 se representa como pares de claves/valores a modo de ejemplo únicamente; la información de credenciales puede estar en cualquier formato no necesariamente limitado a pares de claves/valores.

[0062] La Figura 6 es un diagrama de flujo de un método para proporcionar credenciales de red a modo de ejemplo. En la etapa 602, el servidor de credenciales 116 recibe la solicitud de credenciales del dispositivo digital 102.

[0063] En varios modos de realización, el servidor de credenciales 116 desencripta y autentifica la firma digital con una clave de encriptación. El servidor de credenciales 116 puede entonces identificar un registro de red basándose en el DDID y en el SSID contenidos en el registro de red en la etapa 604. En un ejemplo, el módulo de respuesta a la solicitud de credenciales 206 recupera uno o varios registros de red asociados al DDID en la solicitud de credenciales. El módulo de respuesta a la solicitud de credenciales 206 identifica entonces al menos una credencial de red asociada al SSID en el registro de red recuperado o en los registros de red recuperados.

[0064] En la etapa 606, el módulo de respuesta a la solicitud de credenciales 206 recupera del registro de red seleccionado la(s) credencial(es) de red identificada(s). En un ejemplo, el módulo de respuesta a la solicitud de credenciales 206 identifica un nombre de usuario y una contraseña que el usuario del dispositivo digital 102 debe proporcionar al servidor de autenticación 108 para obtener acceso a la red. El módulo de respuesta a la solicitud de credenciales 206 genera la respuesta a la solicitud de credenciales que comprende las credenciales de red (por ejemplo, nombre de usuario, contraseña) al dispositivo digital 102 en la etapa 608.

[0065] En algunos modos de realización, el módulo de respuesta a la solicitud de credenciales 206 puede identificar la información del procedimiento de acceso como parte de las credenciales de red. El módulo de respuesta a la solicitud de credenciales 206 puede recuperar del registro de red la información del procedimiento de acceso (por ejemplo, el mismo registro de red que contiene una contraseña asociada al SSID). La información del procedimiento de acceso puede contener un identificador de formato e instrucciones (por ejemplo, parámetros) para que el dispositivo digital 102 las siga para obtener acceso a la red. En un ejemplo, el dispositivo digital 102 recupera el identificador de formato y las instrucciones a partir de la credencial de red en la respuesta a la solicitud de credenciales. El dispositivo digital 102 puede identificar formatos recibidos del servidor de autenticación 108 y datos de entrada basándose en el identificador de formato y en las instrucciones. En otro ejemplo, el dispositivo digital 102 proporciona información al servidor de autenticación 108 para obtener acceso a la red basándose en la información del procedimiento de acceso incluida en la respuesta a la solicitud de credenciales.

[0066] La Figura 7 es otro diagrama de flujo del método para proporcionar credenciales de red a modo de ejemplo. El dispositivo digital 102 puede buscar y encontrar una red inalámbrica disponible a través del dispositivo de red 104. Mientras se conecta al punto caliente, el dispositivo digital 102 puede recibir información de configuración de red en la etapa 702. La información de configuración de red puede comprender un identificador del dispositivo de red 104 o el servidor DNS 110. En un ejemplo, el dispositivo digital 102 recibe una dirección IP de servidor DNS (por ejemplo, para el servidor DNS 110) durante el proceso de conexión.

[0067] En la etapa 704, el dispositivo digital 102 genera la solicitud de credenciales. La solicitud de credenciales puede comprender un identificador de secuencia, DDID y SSID. En la etapa 706, el dispositivo digital 102 opcionalmente genera un *nonce* y firma digitalmente la solicitud de credenciales con una clave de encriptación. El dispositivo digital 102 transmite la solicitud de credenciales como un protocolo estándar en la etapa 708. El dispositivo de red 104 puede recibir y remitir la solicitud de credenciales a la red de comunicación 114. En varios modos de realización, el dispositivo de red 104 puede proporcionar la solicitud de credenciales al servidor DNS 110, que puede remitir la solicitud de credenciales al servidor de credenciales 116.

[0068] En modos de realización de ejemplo, el módulo de solicitud de credenciales 204 del servidor de credenciales 116 recibe la solicitud de credenciales. El módulo de solicitud de credenciales 204 puede recuperar del almacenamiento de claves de encriptación 212 una clave de encriptación asociada al DDID en el servidor de credenciales. El módulo de solicitud de credenciales 204 puede entonces desencriptar la firma digital de la solicitud de credenciales para autenticación. El módulo de solicitud de credenciales 204 puede además recuperar de la solicitud de credenciales el *nonce* y un identificador de secuencia.

[0069] El módulo de respuesta a la solicitud de credenciales 206 del servidor de credenciales 116 puede entonces recuperar del almacenamiento de registros de red 210 un registro de red asociado al DDID y al SSID. El módulo de respuesta a la solicitud de credenciales 206 recupera las credenciales de red del registro de red y genera la respuesta a la solicitud de credenciales. La respuesta a la solicitud de credenciales puede comprender las credenciales de red y el *nonce*. El módulo de encriptación/desencriptación 208 puede encriptar la respuesta a la solicitud de credenciales con una clave de encriptación asociada al DDID recuperado del almacenamiento de claves de encriptación 212. En algunos modos de realización, la respuesta a la solicitud de credenciales tiene el formato de un protocolo estándar (por ejemplo, DNS).

[0070] En la etapa 710, el dispositivo digital 102 recibe la respuesta a la solicitud de credenciales. El dispositivo digital 102 posteriormente autentica la respuesta a la solicitud de credenciales en la etapa 712. En un ejemplo, el dispositivo digital 102 desencripta la respuesta a la solicitud de credenciales con la misma clave de encriptación utilizada para firmar digitalmente la solicitud de credenciales. El dispositivo digital 102 puede además recuperar el *nonce* en la respuesta a la solicitud de credenciales y comparar el *nonce* con el *nonce* transmitido en la solicitud de credenciales para autenticación adicional. Si se considera que la respuesta a la solicitud de credenciales es auténtica, el dispositivo digital 102 recupera las credenciales de red a partir de la respuesta a la solicitud de credenciales en la etapa 714.

[0071] En la etapa 716, el dispositivo digital 102 identifica los requisitos de autenticación asociados al acceso a la red. En varios modos de realización, el dispositivo digital 102 determina la información correcta y las credenciales de red para proporcionar al servidor de autenticación 108. En un ejemplo, el dispositivo digital 102 recupera del servidor de autenticación 108 una o varias páginas de acceso a la red. El dispositivo digital 102 puede acceder a la página de acceso a la red correcta del servidor de autenticación y hacer selecciones automáticamente. En un ejemplo, el dispositivo digital 102 puede activar selecciones automáticamente (por ejemplo, activar botones en la página de acceso a la red, casillas de verificación y seleccionar botones de de radio).

[0072] Por ejemplo, el módulo de respuesta a la solicitud de credenciales 206 puede proporcionar instrucciones al dispositivo digital 102 para las selecciones automáticas en una página de acceso a la red. Como se ha mencionado en el presente documento, una página de acceso a la red puede comprender una o varias páginas web, una o varias etiquetas o una combinación de ambas recuperadas del servidor de autenticación 108. En un ejemplo, el *software* en el dispositivo digital 102 puede comprobar automáticamente todas las casillas de selección de una página de acceso a la red. El dispositivo digital 102 puede entonces desmarcar las casillas seleccionadas basándose en la información del procedimiento de acceso. Los expertos en la materia entenderán que puede haber muchos métodos con los que se pueden hacer selecciones de forma automática. En otros modos de realización, el dispositivo digital 102 recibe etiquetas XML del servidor de autenticación 108. El dispositivo digital 102 puede proporcionar información al servidor de autenticación 108 basándose en las etiquetas XML y en las instrucciones de la información del procedimiento de acceso para obtener acceso a la red.

[0073] En la etapa 718, el dispositivo digital 102 proporciona la credencial de red al dispositivo de red 104 para obtener acceso de red a la red de comunicación 114. En un ejemplo, el módulo de respuesta a la solicitud de credenciales 206 recupera uno o varios formularios del servidor de autenticación 108, rellena los formularios con una o varias credenciales de red y proporciona los formularios completados al servidor de autenticación 108. En otro ejemplo, el módulo de respuesta a la solicitud de credenciales 206 proporciona las credenciales de red según sea necesario al servidor de autenticación 108. Una vez que el servidor de autenticación 108 recibe las credenciales de red, el servidor de autenticación 108 puede permitir la comunicación entre el dispositivo digital 102 y la red de comunicación 114. En un ejemplo, el servidor de autenticación 108 ordena al controlador de acceso 112 que permita al dispositivo digital 102 acceder a la red de comunicación 114.

[0074] El dispositivo digital 102 puede posteriormente probar la conectividad de red para confirmar el acceso a la red. En un ejemplo, el dispositivo digital 102 transmite una solicitud al servidor de credenciales 116 para

determinar si la red de comunicación 114 está disponible. En algunos modos de realización, la consulta o mandato contiene el identificador de secuencia previamente enviado en la solicitud de credenciales. Si el acceso a la red se realiza de forma satisfactoria, el servidor de credenciales 116 puede recibir la solicitud y recuperar el identificador de secuencia. El servidor de credenciales 116 puede entonces confirmar que el acceso a la red se realizó de forma satisfactoria.

[0075] La Figura 8 es un diagrama de flujo de un método para recibir y almacenar credenciales de red a modo de ejemplo. En varios modos de realización, los usuarios pueden crear y almacenar registros de red en el servidor de credenciales 116. Por ejemplo, el servidor de credenciales 116 puede comprender un módulo de almacenamiento de credenciales (no se representa) que proporciona una interfaz gráfica de usuario (también conocida como "GUI", del inglés *Graphical User Interface*) que permite a los usuarios crear, almacenar, actualizar, eliminar y modificar registros de red.

[0076] En la etapa 802, el servidor de credenciales 116 proporciona al usuario un formulario de solicitud de credenciales de red. En un ejemplo, el servidor de credenciales 116 proporciona el formulario de solicitud de credenciales de red a un usuario como una o varias páginas web por Internet. El formulario de solicitud de credenciales de red está configurado para recibir el nombre del proveedor de servicios (por ejemplo, el nombre de un operador) y/o el SSID y las credenciales de red.

[0077] El nombre del proveedor de servicios puede comprender el nombre de la entidad que opera el punto caliente, uno o varios componentes relacionados con el punto caliente (por ejemplo, el dispositivo de red 104), o la infraestructura de la red de área local 106. En algunos modos de realización, el nombre del proveedor de servicios comprende el nombre de una organización que gestiona uno o varios puntos calientes para otro proveedor de servicios. En un ejemplo, una cafetería y una librería pueden ambas utilizar un gestor externo para gestionar los puntos calientes, incluso si los puntos calientes tienen diferentes proveedores de servicios. En algunos modos de realización, el formulario de solicitud de credenciales de red se puede configurar para recibir el nombre del gestor externo. En algunos modos de realización, el nombre del proveedor de servicios comprende el nombre de una organización que revende el acceso a una red de punto caliente (por ejemplo, un agregador).

[0078] El formulario de solicitud de credenciales de red también puede recibir el SSID como una selección de servicios de red. En un ejemplo, el formulario de solicitud de credenciales de red comprende un menú desplegable de diferentes proveedores de servicios y/o puntos calientes que el usuario puede seleccionar. Por ejemplo, un usuario puede seleccionar "Starbucks" o "Aeropuerto Internacional de San Francisco" como punto caliente. Al usuario se le pueden dar opciones adicionales como localizaciones geográficas del punto caliente. El usuario puede también seleccionar el proveedor de servicios. Por ejemplo, el usuario puede seleccionar "T-mobile" como proveedor de servicios. El formulario de solicitud de credenciales de red puede entonces permitir al usuario seleccionar uno o varios puntos calientes distintos asociados a T-mobile. La selección o las selecciones se pueden entonces almacenar como un registro de red. De forma alternativa, un identificador de servicio de red asociado a la selección o a las selecciones se genera como el SSID.

[0079] Además, el formulario de solicitud de credenciales de red puede recibir la credencial de red del usuario. Por ejemplo, el usuario puede introducir un nombre de usuario, una contraseña, un código de acceso como credenciales de red en el formulario de solicitud de credenciales de red. En algunos modos de realización, después de que el formulario de solicitud de credenciales de red recibe el SSID, el formulario de solicitud de credenciales de red determina el tipo de credenciales de red requeridas. Por ejemplo, el formulario de solicitud de credenciales de red identifica la información requerida para acceder a una red en un punto caliente en el Aeropuerto Internacional de San Francisco previamente seleccionado por el usuario. El formulario de solicitud de credenciales de red genera entonces campos o selecciones para permitir al usuario introducir sólo la información necesaria (por ejemplo, nombre de usuario, contraseña) para obtener acceso a la red en el punto caliente.

[0080] El servidor de credenciales 116 puede también requerir que el usuario se registre antes de recibir el formulario de solicitud de credenciales de red. Durante el registro, se puede requerir al usuario que acepte las condiciones de servicio y que introduzca la información de cliente. La información de cliente comprende un nombre de usuario y una contraseña para acceder al servidor de credenciales 116 con el fin de almacenar credenciales de red. Opcionalmente, la información de cliente puede comprender la dirección, los datos de contacto y las opciones de pago del usuario para que éste pueda utilizar los servicios que ofrece el servidor de credenciales 116.

[0081] En la etapa 804, el servidor de credenciales 116 recibe la información de cliente y las selecciones de servicio de red mediante el formulario de solicitud de credenciales de red. En la etapa 806, el servidor de credenciales puede recuperar la credencial de red. En la etapa 808, el servidor de credenciales 116 recibe la información de cliente. El servidor de credenciales 116 asocia la credencial de red con la información de cliente, la selección de servicio de red y la(s) credencial(es) de red en la etapa 810 para crear un registro de red. El registro de red se almacena entonces en la etapa 812.

[0082] En algunos modos de realización, el usuario puede acceder de forma manual al servidor de credenciales 116 a través de Internet. En otros modos de realización, el usuario puede descargar e instalar *software* de

credenciales de red en el dispositivo digital 102. El *software* de credenciales de red puede identificar y enviar el DDID del dispositivo digital 102 al servidor de credenciales 116. En otros modos de realización, el *software* de credenciales de red puede estar preinstalado en el dispositivo digital 102. Cuando el dispositivo digital 102 activa por primera vez el *software* de credenciales de red, el *software* de credenciales de red puede identificar y enviar el DDID del dispositivo digital 102 al servidor de credenciales.

[0083] El usuario puede introducir el SSID (por ejemplo, identificar el proveedor de servicios o los puntos calientes) en el *software* de credenciales de red. El usuario puede también introducir las credenciales de red en el *software* de credenciales de red. Después de que el *software* de credenciales de red haya obtenido el DDID, el SSID y las credenciales de red, el *software* de credenciales de red puede subir la información al servidor de credenciales 116, que almacena la información en un registro de red. En varios modos de realización, el *software* de credenciales de red se puede descargar del servidor de credenciales 116.

[0084] La Figura 9 es un de bloques de un dispositivo digital a modo de ejemplo. El servidor de credenciales 116 comprende un procesador 900, un sistema de memoria 902, un sistema de almacenamiento 904, una interfaz I/O (del inglés "*input/output*") 906, una interfaz de red de comunicación 908 y una interfaz de visualización 910. El procesador 900 está configurado para ejecutar instrucciones ejecutables (por ejemplo, programas). En algunos modos de realización, el procesador 900 comprende un sistema de circuitos o cualquier procesador capaz de procesar las instrucciones ejecutables.

[0085] El sistema de memoria 902 es cualquier memoria configurada para almacenar datos. Algunos ejemplos del sistema de memoria 902 son dispositivos de almacenamiento, tales como RAM o ROM. El sistema de memoria 902 puede comprender la RAM caché. En varios modos de realización, los datos se almacenan en el sistema de memoria 902. Los datos en el sistema de memoria 902 se pueden borrar o transferir en última instancia al sistema de almacenamiento 904.

[0086] El sistema de almacenamiento 904 es cualquier almacenamiento configurado para recuperar y almacenar datos. Algunos ejemplos del sistema de almacenamiento 904 son las unidades flash, los discos duros, las unidades ópticas y/o las cintas magnéticas. En algunos modos de realización, el servidor de credenciales 116 incluye un sistema de memoria 902 en forma de RAM y un sistema de almacenamiento 904 en forma de datos flash. Tanto el sistema de memoria 902 como el sistema de almacenamiento 904 comprenden medios legibles por ordenador, que pueden almacenar instrucciones o programas que son ejecutables por una unidad central de procesamiento que incluye el procesador 900.

[0087] La interfaz *input/output* (I/O) opcional 906 es cualquier dispositivo que recibe datos de entrada del usuario y datos de salida. La interfaz de visualización opcional 910 es cualquier dispositivo que se configura para generar gráficos y datos en una pantalla. En un ejemplo, la interfaz de visualización 910 es un adaptador de gráficos. Se entenderá que no todos los dispositivos digitales 102 comprenden la interfaz I/O 906 o la interfaz de visualización 910.

[0088] La interfaz de red de comunicación (interfaz de red de com.) 908 se puede conectar a una red (por ejemplo, la red de área local 106 y la red de comunicación 114) mediante el vínculo 912. La interfaz de red de comunicación 908 puede soportar la comunicación a través de una conexión Ethernet, una conexión en serie, una conexión paralela o una conexión ATA, por ejemplo. La interfaz de red de comunicación 908 también puede soportar comunicación inalámbrica (por ejemplo, 802.11 a/b/g/n, WiMax). Resultará evidente para los expertos en la materia que la interfaz de red de comunicación 908 puede soportar muchos estándares por cable e inalámbricos.

[0089] En varios modos de realización, se describen sistemas y métodos que permiten a un dispositivo digital seleccionar y acceder de forma automática a una red inalámbrica disponible a partir de una multitud de redes inalámbricas disponibles basándose en normas para lograr una calidad de servicio satisfactoria. Dichas normas se podrían implementar en el propio dispositivo digital, en un servidor en comunicación con el dispositivo digital, o en una combinación de los mismos. En varios modos de realización, una red inalámbrica es una red que permite acceso inalámbrico entre un dispositivo digital y una red de comunicación tal como Internet.

[0090] Según varios modos de realización, un usuario de un dispositivo digital inalámbrico (por ejemplo, un dispositivo digital capaz de soportar comunicación wifi) crea una cuenta en un servidor web y registra uno o varios dispositivos digitales (por ejemplo, ordenadores, portátiles, asistentes digitales personales y teléfonos móviles) con esa cuenta. Un servidor central (por ejemplo, un servidor de perfiles o un servidor de credenciales) puede gestionar los dispositivos digitales registrados y aprovisionar un registro de red a través de un mecanismo de comunicación de red, tal como HTTP.

[0091] La Figura 10 es un diagrama de otro entorno en el que se pueden practicar los modos de realización de la presente invención. En varios modos de realización, un usuario con un dispositivo digital 1002 entra en un área situada cerca de los dispositivos de red 1004 y 1006. En un ejemplo, los dispositivos de red 1004 y 1006 son puntos de acceso separados que pueden utilizarse cada uno para establecer comunicación entre el dispositivo digital 1002 y la red de comunicación 1008.

[0092] El dispositivo digital 1002 puede examinar el área circundante al dispositivo digital 1002, detectar los dos dispositivos de red 1004 y 1006 y generar una lista de redes inalámbricas disponibles con las que el dispositivo digital 1002 puede establecer comunicación. En algunos modos de realización, la lista de redes inalámbricas disponibles comprende identificadores DDID, SSID y/o BSID de los dispositivos de red 1004 y 1006.

[0093] Posteriormente, el dispositivo digital 1002 proporciona la lista de redes inalámbricas disponibles a un servidor de normas 1010. En un ejemplo, el dispositivo digital 1002 proporciona la lista de redes inalámbricas disponibles como un protocolo estándar a través de un puerto abierto ya sea del dispositivo de red 1004 o del dispositivo de red 1006 a la red de comunicación 1008 y, por último, al servidor de normas 1010. En otro ejemplo, el dispositivo digital 1002 proporciona la lista de redes inalámbricas disponibles a través de otra red tal como una red de comunicación móvil (por ejemplo, mediante CDMA, GSM, 3G o EVDO) u otra red inalámbrica (por ejemplo, wifi, Wimax o red LTE) no representada.

[0094] El servidor de normas 1010 recibe la lista de redes inalámbricas disponibles y puede recuperar un perfil de red para cada red inalámbrica identificada de la lista. Un perfil de red es un registro que está asociado a una red inalámbrica y que comprende atributos con respecto al rendimiento y/o la calidad de servicio proporcionados por la red asociada. En un ejemplo, el servidor de normas 1010 identifica cada red de la lista y proporciona el SSID y/o el BSID para cada red al servidor de perfiles 1014. El servidor de perfiles 1014 puede entonces proporcionar un perfil de red (basándose en el SSID y/o en el BSID) para cada red al servidor de normas 1010. En algunos modos de realización, el servidor de perfiles 1014 recupera el perfil de red de una base de datos u otro servidor (por ejemplo, un servidor de base de datos de red 1012).

[0095] El servidor de normas 1010 puede seleccionar una red inalámbrica preferida de la lista de redes inalámbricas disponibles basándose en los atributos de los perfiles de red y/o en cualquier atributo recibido desde el dispositivo digital 1002. Un atributo es una característica de una red inalámbrica. En varios modos de realización, un atributo incluye una medición de rendimiento, un indicador de compartido o un identificador de servicio. Una medición de rendimiento de una red inalámbrica es cualquier medida del rendimiento de la red. En algunos ejemplos, una medición de rendimiento puede comprender una medición de latencia, una medición de ancho de banda o una medición de calidad de servicio. Los expertos en la materia entenderán que una medición de rendimiento puede incluir cualquier tipo de medición que represente el rendimiento de una red inalámbrica.

[0096] Una medición de latencia es una medida que representa el tiempo para enviar un paquete de datos desde el dispositivo digital hasta un servidor en una red. En algunos modos de realización, el dispositivo digital 1002 puede enviar un paquete de “petición eco” ICMP (ICMP = Protocolo de Mensajes de Control de Internet) a un servidor y esperar una contestación de “respuesta eco” ICPM. La medida de latencia puede comprender una estimación del tiempo de ida y vuelta (generalmente en milisegundos) y/o incluir cualquier pérdida de paquete. En otro ejemplo, la medición de latencia es la mitad del tiempo de ida y vuelta estimado.

[0097] Una medición de ancho de banda es una medida del ancho de banda disponible de una red inalámbrica. En un ejemplo, el dispositivo digital puede comprobar el ancho de banda disponible enviando un bloque de datos por la red inalámbrica a un servidor y midiendo el tiempo de la respuesta.

[0098] Una medición de calidad de servicio es cualquier medición que mida la calidad de servicio de la red inalámbrica, del dispositivo de acceso 1004, del dispositivo de acceso 1006 y/o de la red de comunicación 1008. En un ejemplo, la medición de calidad de servicio representa una fiabilidad del DHCP que se determina midiendo la cantidad de tiempo necesaria para obtener una dirección IP. La fiabilidad del DHCP puede comprender una medida estadística, una probabilidad de recibir una dirección IP y/o una distribución de tiempo.

[0099] Un indicador de compartido indica si se comparte una red inalámbrica. En algunos modos de realización, el indicador de compartido puede ser uno de tres estados incluyendo “compartida”, “no compartida” y “desconocida”. Aunque el indicador de compartido pueda incluir sólo un único estado (por ejemplo, “no compartida”), los expertos en la materia entenderán que el indicador de compartido puede tener cualquier número de estados. Una red inalámbrica con un indicador de compartido que indica que la red está “compartida” puede indicar que el propietario de la red inalámbrica tiene la intención de que otros utilicen la red. Un ejemplo de una red “compartida” puede incluir una red inalámbrica que está intencionalmente “abierta” (por ejemplo, sin encriptar) para que otros la utilicen.

[0100] Una red inalámbrica con un indicador de compartido que indica que la red está “no compartida” puede indicar que el propietario de la red inalámbrica no desea que cualquier persona que no tenga autorización expresa acceda a la red. En un ejemplo, las redes inalámbricas que no están compartidas a menudo se encriptan intencionadamente (por ejemplo, mediante WEP o WPA) para limitar el acceso a usuarios no autorizados. No obstante, no todas las redes que son “no compartidas” están encriptadas. Por ejemplo, el propietario de la red puede configurar mal el dispositivo de red o, por error, permitir que una red esté abierta (es decir, sin encriptar) aunque no se pretenda compartir la red.

[0101] Una red inalámbrica con un indicador de compartido que indica que la red es “desconocida” puede indicar que la red inalámbrica puede ser o “compartida” o “no compartida”. Por ejemplo, la intención del dueño de una red abierta puede no conocerse.

[0102] Un identificador de servicios puede identificar uno o varios servicios soportados por la red inalámbrica. En un ejemplo, uno o varios identificadores de servicios indican que una red inalámbrica soporta Voz sobre Protocolo de Internet (VOIP, por sus siglas en ingles *Voice over IP*), teleconferencias y/o videoconferencias. El identificador de servicios puede identificar cualquier tipo de servicio que la red inalámbrica soporta. En algunos modos de realización, el identificador de servicios puede identificar servicios que la red inalámbrica no soporta.

[0103] Los expertos en la materia entenderán que el perfil de red puede comprender cualquier número de atributos. Además, los expertos en la materia entenderán que el perfil de red puede comprender sólo una o varias mediciones de rendimiento, sólo un indicador de compartido o sólo uno o varios identificadores de servicios.

[0104] En varios modos de realización, el servidor de normas 1010 selecciona una o varias redes inalámbricas de la lista de redes inalámbricas disponibles basándose en el análisis de atributos. En un ejemplo, el servidor de normas 1010 aplica normas a los atributos. Las reglas pueden comprender requisitos mínimos, configuraciones personalizadas y comparaciones de atributos. En un ejemplo, las normas aplicadas por el servidor de normas 1010 pueden comparar los atributos de una o varias redes inalámbricas con uno o varios requisitos mínimos. Si los atributos de una red inalámbrica están por debajo de los requisitos mínimos, entonces la red inalámbrica puede no seleccionarse o eliminarse de la lista de redes inalámbricas disponibles.

[0105] En algunos modos de realización, las normas que aplica el servidor de normas 1010 se pueden basar en configuraciones personalizadas del usuario. Por ejemplo, el usuario del dispositivo digital 1002 puede indicar una configuración personalizada que indica que el dispositivo digital 1002 sólo se puede conectar mediante redes inalámbricas que han sido designadas como “compartidas”. En este ejemplo, el servidor de normas 1010 puede seleccionar únicamente aquellas redes inalámbricas con un atributo que comprende un indicador de compartido que identifica la red inalámbrica como “compartida”.

[0106] En varios modos de realización, las normas que el servidor de normas 1010 aplica se pueden basar en una comparación de los atributos de una red inalámbrica con otra. En un ejemplo, los atributos pueden indicar que una red inalámbrica tiene un ancho de banda mayor y una latencia menor que otra. En este ejemplo, el servidor de normas 1010 puede seleccionar una red inalámbrica que tiene mejor rendimiento o servicios valiosos en comparación con otra. Los expertos en la materia entenderán que se puede utilizar cualquier tipo de norma para seleccionar o asistir en la selección de una red inalámbrica de la lista de redes inalámbricas disponibles.

[0107] El servidor de normas 1010 puede aplicar más de una norma a la hora de seleccionar una red inalámbrica. En un ejemplo, el servidor de normas 1010 puede aplicar una configuración personalizada del usuario antes de comparar los atributos de diferentes redes inalámbricas y hacer una selección. En otro ejemplo, el servidor de normas 1010 puede aplicar requisitos mínimos a los atributos antes de comparar los atributos.

[0108] Una vez que el servidor de normas 1010 selecciona la red inalámbrica basándose en la comparación de atributos de los perfiles de red, el servidor de normas 1010 puede proporcionar la selección de red inalámbrica al dispositivo digital 1002. Una selección de red inalámbrica incluye uno o varios identificadores (por ejemplo, identificadores de red) que identifican al menos una red inalámbrica. La selección de red inalámbrica puede identificar una única red inalámbrica o comprender una lista ordenada de redes inalámbricas que se ordena en función del orden de preferencia.

[0109] En algunos modos de realización, el servidor de normas 1010 proporciona credenciales (por ejemplo, una respuesta a una solicitud de credenciales) para la red inalámbrica seleccionada además de la selección de red inalámbrica del dispositivo digital 1002. En un ejemplo, el servidor de normas 1010 proporciona la red inalámbrica seleccionada al servidor de credenciales 1016, que entonces proporciona al dispositivo digital 1002 una respuesta a una solicitud de credenciales (aunque no se ha hecho ninguna solicitud de credenciales) para la red inalámbrica seleccionada. En otros modos de realización, el dispositivo digital 1002 recibe la selección de red inalámbrica y entonces procede a transmitir una solicitud de credenciales al servidor de credenciales 1016 para recibir las credenciales como se describe en el presente documento.

[0110] Además, en varios modos de realización, el dispositivo digital 1002 intenta establecer una conexión basándose en la red inalámbrica seleccionada. Si la conexión falla, el dispositivo digital 1002 puede transmitir una solicitud de credenciales al servidor de credenciales 1016 para recuperar las credenciales para acceder a la red como se describe en el presente documento. El dispositivo digital 1002 puede proporcionar la solicitud de credenciales al servidor de credenciales 1016 a través de un puerto abierto del dispositivo de red 1004. En otro ejemplo, el dispositivo digital 1002 puede proporcionar una solicitud de credenciales a través de cualquier otra red que incluya una conexión con un dispositivo de red diferente o a través de una conexión móvil.

[0111] Aunque el servidor de normas 1010, el servidor de base de datos de red 1012, el servidor de perfiles 1014, el servidor de credenciales 1016 y el servidor web 1018 se representan como servidores independientes en la Figura 1, los servidores pueden estar todos combinados en uno o varios servidores. De forma similar, las funciones de cualquiera de los servidores las puede llevar a cabo uno de los otros servidores representados o cualquier otro servidor.

[0112] Aunque la Figura 10 representa varios servidores (por ejemplo, servidor de normas, servidor de base de datos de red, servidor de perfiles, servidor de credenciales y servidor web) para llevar a cabo la selección de una red inalámbrica a partir de la multitud de redes inalámbricas disponibles, los expertos en la materia entenderán que la selección de las redes inalámbricas puede tener lugar en el dispositivo digital 1002. En un ejemplo, el dispositivo digital 1002 recupera los resultados examinados que listan las redes inalámbricas disponibles y selecciona una red inalámbrica basándose en las preferencias de configuración. Las preferencias de configuración se pueden basar en una o varias normas ejecutadas localmente, en la intensidad de señal preferida o en cualquier otro atributo o atributos. En otro ejemplo, el dispositivo digital 1002 selecciona una red inalámbrica que soporta un servicio deseado (por ejemplo, VOIP), cumple un estándar de latencia mínimo y cumple un estándar de calidad de servicio mínimo. En otro ejemplo, el servidor de perfiles 1014 proporciona los perfiles de red deseados al dispositivo digital 1002, que realiza el análisis para determinar la red inalámbrica preferida.

[0113] La Figura 11 es un diagrama de flujo de un proceso para proporcionar una selección de una red inalámbrica a modo de ejemplo. En la etapa 1102, un servidor (por ejemplo, un servidor de normas 1010, un servidor de base de datos de red 1012, un servidor de perfiles 1014, un servidor de credenciales 1016 o un servidor web 1018) recibe una lista de redes inalámbricas disponibles del dispositivo digital 1002. En algunos ejemplos, la lista comprende los SSIDs y los BSIDs de uno o varios dispositivos de red (por ejemplo, el dispositivo de red 1004 y el dispositivo de red 1006). La lista puede comprender cualquier información que identifique una red y/o un dispositivo de red.

[0114] En algunos modos de realización, el servidor también recibe uno o varios atributos asociados a una red y/o a un dispositivo de red. En varios modos de realización, el dispositivo digital 1002 mide la intensidad de la señal, determina los servicios disponibles o toma una medición de rendimiento de una o varias redes y/o dispositivos de red que están identificados en la lista de redes inalámbricas disponibles.

[0115] En la etapa 1104, el servidor recupera un perfil de red de una multitud de perfiles de red almacenados en una base de datos de red para cada red inalámbrica disponible de la lista de redes inalámbricas disponibles. Cada perfil de red puede comprender al menos un atributo. En algunos modos de realización, no todas las redes inalámbricas de la lista tienen un perfil de red. Cuando no se encuentra un perfil de red para una red inalámbrica de la lista, un perfil de red asociado a la red inalámbrica puede crearse entonces. Si los atributos se reciben del dispositivo digital 1002, el servidor puede determinar qué atributo recibido del dispositivo digital 1002 está asociado a qué red, dispositivo de red y/o perfil de red.

[0116] En la etapa 1106, el servidor compara los atributos de cada perfil de red con los requisitos mínimos. En un ejemplo, el servidor compara las mediciones de latencia de todos los perfiles de red de la lista (si están disponibles) con una medición de latencia mínima. El servidor también puede comparar los atributos recibidos del dispositivo digital 1002 con los requisitos mínimos. En la etapa 1108, el servidor elimina una o varias redes inalámbricas de la lista de redes inalámbricas disponibles y/o perfiles de redes inalámbricas basándose en la comparación o en las comparaciones. Por ejemplo, cualquier red inalámbrica con una medición de latencia por debajo de la medición de latencia mínima no se puede seleccionar. En otros modos de realización, una red inalámbrica con una medición de latencia por debajo de la medición de latencia mínima puede recibir un valor ponderado que se comparará con otras redes inalámbricas para ayudar en el proceso de selección.

[0117] En algunos modos de realización, el usuario del dispositivo digital 1010 determina los requisitos mínimos. En otros modos de realización, los requisitos mínimos pueden ser elegidos para el usuario (por ejemplo, por un administrador).

[0118] En la etapa 1110, el servidor recupera la configuración personalizada para un usuario. El usuario puede enviar la configuración personalizada al servidor. En algunos modos de realización, el usuario tiene una cuenta con el servidor web 1018 que contiene las configuraciones personalizadas. En un ejemplo, el servidor recibe un identificador de usuario junto con la lista de redes inalámbricas disponibles. El servidor accede entonces a la cuenta del usuario y recibe la configuración personalizada que se aplica entonces a los atributos de los perfiles de red asociados a una red inalámbrica de la lista. En varios modos de realización, los usuarios pueden establecer una configuración personalizada (por ejemplo, la “agresividad”) en la que un dispositivo digital 1002 puede conectarse a una red inalámbrica. Dicha configuración podría incluir:

(a) Conectarse a cualquier red abierta, independientemente del indicador de compartido;

(b) conectarse a cualquier red abierta, exceptuando aquéllas con SSIDs del fabricante por defecto (por ejemplo, “linksys”) que probablemente indican que el propietario simplemente dejó el punto de acceso abierto por defecto y desconoce cómo configurar las funciones de seguridad;

(c) conectarse a cualquier red abierta que el servidor de perfiles 108 haya visto (o información almacenada sobre la red wifi); o

(d) conectarse a cualquier red abierta con un indicador de compartido que indique “compartida”, o se ha indicado como compartida por algún otro medio.

Los expertos en la materia entenderán que puede haber muchas configuraciones personalizadas.

[0119] En la etapa 1112, el servidor elimina una o varias redes inalámbricas de la lista o perfiles de red basándose en la configuración personalizada. Por ejemplo, la configuración personalizada puede indicar que el usuario sólo desea conectar a redes inalámbricas que soportan videoconferencias y mantener un requisito de calidad de servicio definido por el usuario. El servidor puede entonces eliminar cualquier red inalámbrica de la lista de redes inalámbricas disponibles que no cumple la configuración personalizada del usuario basándose en los atributos de los perfiles de red o en los recibidos recientemente del dispositivo digital 1002.

[0120] En algunos modos de realización, la configuración personalizada puede entonces tenerse en cuenta antes o después de la comparación de los atributos de los perfiles de red. En un ejemplo, la configuración personalizada indica que el usuario no desea conectarse a una red inalámbrica que no está designada como “compartida” o que proporciona ciertos servicios. En un ejemplo, el servidor de normas 1010 tampoco recupera los perfiles de red asociados a las redes que no proporcionan el servicio necesario y/o no comparan los atributos asociados a esas redes. En otros modos de realización, el dispositivo digital 1002 aplica una configuración personalizada a los resultados (por ejemplo, la selección de red inalámbrica) recibidos del servidor de normas 1010 antes de acceder a una red inalámbrica preferida.

[0121] En la etapa 1114, el servidor compara los atributos de las redes inalámbricas que quedan en la lista. En varios modos de realización, el servidor aplicará una ponderación y normalizará uno o varios de los atributos (por ejemplo, las mediciones) procedentes de los perfiles de red. En algunos modos de realización, los atributos más antiguos se pueden eliminar o ponderarse menos que otros atributos que son nuevos. En un ejemplo, cualquier medición que tiene más de una semana puede recibir menos ponderación que una medición similar nueva. En otro ejemplo, una medición que tiene más de un mes se puede eliminar de los perfiles de red o no considerarse en la comparación. Los expertos en la materia entenderán que no todos los atributos o información procedente de los perfiles de red pueden considerarse en la comparación.

[0122] Cada perfil de red puede comprender cualquier número de atributos. En un ejemplo, el servidor de normas 1010 realiza una selección de red inalámbrica basándose en la comparación de una medición de dos perfiles de red diferentes. En algunos modos de realización, el servidor de normas 1010 selecciona una red inalámbrica basándose en una comparación entre dos mediciones similares (es decir, la medición de latencia del primer perfil de red se compara con la medición de latencia del segundo perfil de red). Los expertos en la materia entenderán que el servidor de normas 1010 puede seleccionar una red inalámbrica basándose en las comparaciones entre dos mediciones similares recibidas recientemente o una medición recibida recientemente y otra de un perfil de red.

[0123] En otros modos de realización, el servidor de normas 1010 selecciona una red inalámbrica basándose en una comparación de dos mediciones diferentes (por ejemplo, la medición de latencia del primer perfil de red se compara con una medición del ancho de banda del segundo perfil de red). El servidor de normas 1010 puede ejecutar un algoritmo para ponderar y normalizar mediciones o atributos similares y/o diferentes con el fin de realizar una comparación para seleccionar la red inalámbrica apropiada. En un ejemplo, el servidor de normas 1010 compara una medición de latencia en el primer perfil de red con una medición del ancho de banda en el segundo perfil de red. El servidor de normas 1010 puede ejecutar un algoritmo para ponderar y normalizar las mediciones. El algoritmo puede ponderar la medición de latencia en mayor medida que la medición del ancho de banda, puesto que la latencia puede tener un mayor impacto en el rendimiento de la red.

[0124] Un atributo o una medición pueden recibir ponderaciones diferentes dependiendo de varios de factores. Por ejemplo, una medición de latencia puede recibir una ponderación dada cuando la medición se encuentra en un rango aceptable, de lo contrario la medición de latencia puede ser significativamente menos ponderada. Una medición recibida del dispositivo digital 1002 recientemente puede recibir una mayor ponderación que una medición similar de un perfil de red. Los expertos en la materia entenderán que hay muchas maneras de comparar mediciones cualitativas y/o de rendimiento similares y/o diferentes.

[0125] En la etapa 1116, el servidor selecciona una red inalámbrica basándose en la comparación de atributos. La selección de la red inalámbrica puede comprender una única red inalámbrica preferida o una lista de redes inalámbricas ordenadas en función del orden de preferencia. En un ejemplo, el servidor de normas 1010

identifica la red más preferida, la segunda red más preferida, etcétera. El servidor de normas 1010 proporciona entonces la selección de la red inalámbrica al dispositivo digital 1002 en la etapa 1118.

[0126] En varios modos de realización, el servidor de normas 1010 sólo compara mediciones que se han recibido recientemente del dispositivo digital 1002. En un ejemplo, se reciben del dispositivo digital 1002 dos mediciones de latencia. Cada medición de latencia se asocia a una red inalámbrica distinta identificada en una lista de redes disponibles. En este ejemplo, el servidor de normas 1010 puede seleccionar una red inalámbrica basándose en una comparación de los dos atributos.

[0127] La Figura 12 es un diagrama de flujo de un proceso para seleccionar una red inalámbrica a modo de ejemplo. En la etapa 1002, el dispositivo digital 1002 entra en un área con dos redes inalámbricas y el dispositivo digital 1202 busca redes a las que acceder. En la etapa 1204, el dispositivo digital 1002 recibe un primer y un segundo identificador de red de redes inalámbricas disponibles. Como se describe en el presente documento, el primer y el segundo identificador de red pueden comprender BSIDs, SSIDs o cualquier otro identificador de red. Por ejemplo, el primer identificador de red puede comprender un identificador BSID y el segundo identificador de red puede comprender un identificador SSID. En otro ejemplo, la primera red puede proporcionar varios identificadores incluyendo un BSID y un SSID mientras que la segunda red proporciona sólo un SSID. En este ejemplo, el primer identificador de red puede comprender tanto el BSID como el SSID del primer dispositivo de red mientras que el segundo identificador de red sólo es un SSID del segundo dispositivo de red.

[0128] En la etapa 1206, el dispositivo digital 1002 genera una lista de redes inalámbricas disponibles. Por ejemplo, el dispositivo digital 1002 puede generar una lista que comprende el primer identificador de red y el segundo identificador de red. La lista se proporciona entonces a un servidor en la etapa 1208.

[0129] En la etapa 1210, el dispositivo digital 1002 recibe del servidor una selección de red inalámbrica. La selección de red inalámbrica puede comprender un identificador que identifica la red inalámbrica seleccionada o que identifica el dispositivo de red asociado a la red inalámbrica seleccionada (por ejemplo, un BSID y/o un SSID del dispositivo de red). En varios modos de realización, la selección de red inalámbrica puede comprender una lista de redes inalámbricas ordenadas por preferencia. La lista puede comprender dos o varios identificadores que identifican una red inalámbrica seleccionada o un dispositivo de red.

[0130] En la etapa 1212, el dispositivo digital 1002 recibe del servidor credenciales para la selección de la red inalámbrica. En algunos modos de realización, las credenciales se reciben del mismo servidor que recibió la lista de redes inalámbricas disponibles del dispositivo digital 1002.

[0131] En varios modos de realización, el dispositivo digital 1002 recibe del servidor la selección de red inalámbrica y proporciona entonces una solicitud de credenciales con el fin de recibir las credenciales para la red deseada. En un ejemplo, el dispositivo digital 1002 proporciona la solicitud de credenciales de la misma manera que el dispositivo digital 1002 proporcionó la lista de redes inalámbricas disponibles (por ejemplo, a través de un puerto abierto de una red). En algunos modos de realización, la red preferida no requiere credenciales o las credenciales están almacenadas localmente en el dispositivo digital 1002.

[0132] En la etapa 1214, el dispositivo digital 1002 accede a la red inalámbrica seleccionada con las credenciales. El proceso para aplicar las credenciales a una página de acceso o similar se describe en el presente documento.

[0133] En varios modos de realización, el dispositivo digital 1002 puede proporcionar la lista de redes inalámbricas disponibles al servidor a través de un puerto abierto de un dispositivo de red de forma similar a proporcionar una solicitud de credenciales descrita en el presente documento. En otros modos de realización, el dispositivo digital 1002 puede proporcionar la lista al servidor a través de otra red. En un ejemplo, el dispositivo digital 1002 genera una lista de redes wifi disponibles y proporciona la lista a través de una red móvil (por ejemplo, una red EV-DO, o HSDPA). En este ejemplo, la selección de red inalámbrica se puede devolver al dispositivo digital a través de la red móvil y entonces el dispositivo digital 1002 puede intentar acceder a la red wifi preferida.

[0134] En otro ejemplo, el dispositivo digital 1002 accede a una red inalámbrica. El dispositivo digital 1002 puede entonces proporcionar una lista de las redes inalámbricas disponibles al servidor. El servidor puede devolver la selección de red inalámbrica al dispositivo digital 1002. Si la red inalámbrica preferida no es la red a la que el dispositivo digital 1002 ha accedido originalmente, entonces el dispositivo digital 1002 puede interrumpir la conexión y acceder a la red inalámbrica preferida.

[0135] Aunque las Figuras 10-12 contemplan un servidor que recibe una lista de redes inalámbricas disponibles, que determina una selección de red inalámbrica y que proporciona la selección al dispositivo digital 1002, los expertos en la materia entenderán que no es necesario un servidor. En un ejemplo, el dispositivo digital 1002 genera una lista de redes inalámbricas disponibles y entonces recupera cualquier información disponible sobre las redes de la lista (por ejemplo, de perfiles de red almacenados localmente, de uno o varios dispositivos de red, de una base de datos local o remota y/o recupera información de otra red como Internet). El dispositivo digital

1002 puede entonces realizar comparaciones basándose en qué atributos asociados a las redes están disponibles para realizar una selección o generar una lista priorizada. El dispositivo digital 1002 puede entonces acceder a la red inalámbrica seleccionada.

[0136] En varios modos de realización, el dispositivo digital 1002 puede generar y proporcionar atributos sobre una o varias redes para actualizar los perfiles de red. En un ejemplo, el dispositivo digital 1002 determina la calidad de la señal, el ancho de banda o cualquier otra medición y proporciona esas mediciones junto con la lista de redes inalámbricas disponibles a un servidor. En otro ejemplo, conforme el dispositivo digital 1002 accede a una red inalámbrica seleccionada, mide atributos y proporciona las mediciones de actualización de atributos en un perfil de red. El dispositivo digital 1002 puede tomar los atributos (por ejemplo, mediciones de latencia, mediciones de ancho de banda y mediciones de calidad de servicio) en cualquier momento y utilizarlos para actualizar los perfiles de red.

[0137] La Figura 13 es un diagrama para seleccionar una red inalámbrica y acceder a la red inalámbrica seleccionada. En varios modos de realización, el dispositivo de red 1004 y el dispositivo de red 1006 proporcionan un primer y un segundo identificador de red al dispositivo digital 1002 en las etapas 1302 y 1304. En la etapa 1306, el dispositivo digital 1002 genera mediciones (es decir, atributos) tomando medidas sobre las redes inalámbricas asociadas al dispositivo de red 1004 y al dispositivo de red 1006. En algunos ejemplos, las mediciones pueden incluir mediciones de latencia, de intensidad de señal o de calidad de servicio.

[0138] En la etapa 1308, el dispositivo digital 1002 genera una lista de redes inalámbricas disponibles que puede incluir el identificador de red del dispositivo red 1004, así como el identificador de red del dispositivo de red 1006. En algunos modos de realización, el dispositivo digital 1002 puede comprender también una configuración personalizada que puede indicar una preferencia entre los dos identificadores de red o eliminar uno o ambos identificadores de red. En un ejemplo, la configuración personalizada indica que sólo se puede acceder a redes abiertas que no tienen un SSID del fabricante por defecto (por ejemplo, “linksys”). En este ejemplo, si el identificador de red del dispositivo de red 1004 indica un SSID del fabricante por defecto, el dispositivo digital 1002 puede no incluir ese identificador de red para el dispositivo de red 1004 en la lista de redes inalámbricas disponibles.

[0139] En algunos modos de realización, si el dispositivo digital 1002 no puede generar una lista que identifique al menos dos o más redes, el dispositivo digital 1002 no envía la lista. En un ejemplo, si el dispositivo digital 1002 sólo puede identificar una red inalámbrica disponible que cumple los requisitos del usuario, entonces el dispositivo digital 1002 puede intentar acceder a la red inalámbrica directamente o enviar una solicitud de credenciales a un servidor para recuperar cualquier credencial necesaria para el acceso.

[0140] En la etapa 1310, el dispositivo digital 1002 proporciona los atributos y la lista de redes inalámbricas disponibles a través de un puerto abierto (por ejemplo, puerto 53) del dispositivo de red 1006, que actúa como un proxy al proporcionar los atributos y la lista de redes inalámbricas disponibles al servidor de normas 1010. En otros modos de realización, el dispositivo digital 1002 proporciona los atributos y la lista a través de un puerto abierto del dispositivo de red 1004. De forma alternativa, el dispositivo digital 1002 puede proporcionar los atributos y la lista a través de redes distintas (por ejemplo, los atributos a través de un puerto abierto de uno de los dispositivos de red y la lista a través de una red móvil). En la etapa 1312, el dispositivo de red 1006 actúa como un proxy proporcionando los atributos y la lista mediante DNS al servidor de normas 1010.

[0141] En la etapa 1314, el servidor de normas 1010 recupera perfiles de red. En un ejemplo, el servidor de normas 1010 recupera de la lista los identificadores de red y recupera los perfiles de red asociados a los identificadores de red.

[0142] En la etapa 1316, el servidor de normas 1010 (o el servidor de perfiles 1014) actualiza atributos en los perfiles de red con los atributos recibidos del dispositivo digital 1002. En un ejemplo, se utiliza una medición de latencia nueva procedente del dispositivo digital 1002 para actualizar el perfil de red asociado al identificador de red procedente del dispositivo de red 1004. También se puede actualizar un valor del período de vida asociado al atributo para indicar que la medición de latencia nueva es reciente.

[0143] En la etapa 1318, el servidor de normas 1010 selecciona un dispositivo de red basándose en la comparación de atributos procedentes de los perfiles de red. En algunos modos de realización, el servidor de normas 1010 también aplica una configuración personalizada procedente del dispositivo digital 1002 o de una cuenta asociada al dispositivo digital 1002 (por ejemplo, mediante el servidor web 1018) antes de realizar una selección. El servidor de normas 1010 puede preparar una lista priorizada de los dos dispositivos de red a partir de la lista proporcionada por el dispositivo digital 1002. La lista se prioriza basándose en cuál de los dos dispositivos de red proporciona el servicio más deseable basándose en las mediciones de los perfiles de red.

[0144] En la etapa 1320, el servidor de normas 1010, proporciona la selección de redes inalámbricas y las credenciales mediante DNS de vuelta al dispositivo de red 1006 con el fin de que funcione como un proxy para enviar la información al dispositivo digital 1002. En un ejemplo, el servidor de normas 1010 selecciona el dispositivo de red 1004. El servidor de normas 1010 puede recuperar las credenciales para el dispositivo de red

1004 basándose en el identificador de red del dispositivo de red 1004. Por ejemplo, el servidor de normas 1010 puede proporcionar una solicitud de credenciales al servidor de credenciales 1016. El servidor de credenciales 1016 puede proporcionar una respuesta a una solicitud de credenciales que contiene las credenciales necesarias para el servidor de normas 1010, que envía entonces las credenciales recibidas del servidor de credenciales 1016, así como la selección de red inalámbrica al dispositivo digital 1002.

[0145] En la etapa 1322, entonces el dispositivo de red 1006 proporciona la selección de red y las credenciales por el puerto abierto al dispositivo digital 1002. En la etapa 1324, el dispositivo digital 1002 proporciona las credenciales para acceder al dispositivo de red 1004 y genera atributos adicionales con respecto a la red (es decir, toma medidas adicionales). Una vez que se establece una conexión, se proporcionan los atributos nuevos al servidor de normas 1010 o al servidor de perfiles 1014 para actualizar el perfil de red asociado al dispositivo de red 1004 en la etapa 1326. En un ejemplo, el dispositivo digital 1002 puede medir el tiempo necesario para establecer la conexión con el dispositivo de red 1004. El tiempo necesario para establecer la conexión puede entonces utilizarse para actualizar los atributos en un perfil de red. Si no se establece una conexión o falla la conexión, esa información puede proporcionarse también para actualizar el perfil de red asociado.

[0146] En algunos modos de realización, si la conexión de red con la red seleccionada falla, el dispositivo digital 1002 puede reintentar establecer la conexión. Si fallan varios intentos por establecer la conexión, se envía información sobre el fallo para actualizar el perfil de red asociado. El dispositivo digital 1002 puede entonces intentar establecer una conexión con otro dispositivo de red (por ejemplo, el dispositivo de red 1006). En algunos modos de realización, el dispositivo digital 1002 vuelve a explorar el área y genera una nueva lista de redes disponibles que puede no incluir la red que a la que el dispositivo digital 1002 no consiguió conectar. La nueva lista se puede enviar al servidor de normas 1010 para recibir una nueva selección de red inalámbrica y el proceso se puede repetir.

[0147] En algunos modos de realización, el servidor de normas 1010 proporciona una lista priorizada de redes inalámbricas disponibles ordenadas por preferencia. En un ejemplo, el servidor de normas 1010 proporciona una lista priorizada de tres redes al dispositivo digital 1002. El dispositivo digital 1002 puede entonces intentar acceder a la primera red inalámbrica de la lista priorizada. Si el dispositivo digital 1002 no puede conectar a la primera red inalámbrica, entonces el dispositivo digital 1002 puede proceder a intentar conectar a la siguiente red de la lista. Los expertos en la materia entenderán que la lista priorizada puede contener todas, una o alguna de las redes inalámbricas identificadas en la lista de redes inalámbricas disponibles. Por ejemplo, el servidor de normas 1010 puede no identificar redes inalámbricas que se sabe que ofrecen un rendimiento pobre, que no proporcionan el servicio deseado (por ejemplo, servicio VOIP) y/o que están restringidas de otra manera.

[0148] En varios modos de realización, el usuario del dispositivo digital 1002 puede anular la selección de red inalámbrica para acceder a cualquier red inalámbrica. En un ejemplo, el usuario elige la prioridad de las redes inalámbricas disponibles. En algunos modos de realización, el usuario puede configurar el dispositivo digital 1002 o configurar una cuenta con el servidor web 1018 para incluir preferencias personales que pueden reordenar o alterar de otra manera una lista priorizada de redes inalámbricas procedente del servidor de normas 1010. Por ejemplo, el dispositivo digital 1002 o el servidor web 1018 pueden alterar la lista de redes inalámbricas disponibles basándose en las preferencias del usuario antes de proporcionársela al servidor de normas 1010.

[0149] En algunos modos de realización, además de una o varias redes wifi abiertas, también puede haber una o varias redes wifi encriptadas en una ubicación determinada. Un dispositivo digital 1002 puede conectar a una red wifi abierta y transmitir el SSID de otras redes wifi, incluyendo redes wifi encriptadas, al servidor de normas 1010 mediante un protocolo de comunicación de red tal como HTTP.

[0150] El servidor de normas 1010 puede entonces determinar, basándose en la configuración personalizada o en otras normas, que una red wifi encriptada disponible es la elección preferida para una conexión de red. El servidor de normas 1010 puede transmitir las claves de encriptación necesarias al dispositivo digital 1002 por la conexión de red wifi abierta actual y enviar las instrucciones al dispositivo digital 1002 para cambiar a la red wifi encriptada.

[0151] Las funciones y los componentes previamente descritos pueden comprender instrucciones que se almacenan en un soporte de almacenamiento tal como un soporte legible por ordenador. Un procesador puede recuperar y ejecutar las instrucciones. Algunos ejemplos de instrucciones son *software*, código de programa y *firmware*. Algunos ejemplos de soporte de almacenamiento son dispositivos de memoria, cintas, discos, circuitos integrados y servidores. Las instrucciones están operativas cuando las ejecuta el procesador para dirigir al procesador con el fin operar según modos de realización de la presente invención. Los expertos en la materia están familiarizados con las instrucciones, el procesador o los procesadores y el soporte de almacenamiento.

[0152] La presente invención se describe previamente con referencia a modos de realización de ejemplo. Resultará evidente para los expertos en la materia que se pueden realizar varias modificaciones y que se pueden utilizar otros modos de realización sin alejarse del alcance más amplio de la presente invención. Por consiguiente, la presente invención pretende cubrir estas y otras variaciones sobre los modos de realización de ejemplo.

REIVINDICACIONES

1. Un método que comprende:

recibir (1102), mediante un servidor (1010) procedente de un dispositivo digital (1002), un primer identificador de dispositivo de red para un primer dispositivo de red (1004) que da acceso a una primera red, y un segundo identificador de dispositivo de red para un segundo dispositivo de red (1006) que da acceso a una segunda red;

recuperar (1104), mediante el servidor (1010), un primer perfil de red que comprende un primer atributo, basándose el primer perfil de red en el primer identificador de dispositivo de red;

recuperar (1104), mediante el servidor (1010), un segundo perfil de red que comprende un segundo atributo, basándose el segundo perfil de red en el segundo identificador de dispositivo de red;

seleccionar (1116), mediante el servidor (1010), o el primer identificador de dispositivo de red o el segundo identificador de dispositivo de red basándose en un análisis de atributo del primer atributo y del segundo atributo, estando el identificador de dispositivo de red seleccionado asociado al primer o al segundo dispositivo de red con el fin de permitir al dispositivo digital seleccionar el primer o el segundo dispositivo de red para acceder a la primera o a la segunda red basándose en la selección; y

proporcionar, mediante el servidor (1010), un identificador de selección de red inalámbrica al dispositivo digital (1002), basándose en la selección, estando el identificador de selección de red inalámbrica asociado al primer dispositivo de red (1004) o al segundo dispositivo de red (1006) para permitir al dispositivo digital (1002) iniciar un acceso con el primer dispositivo de red asociado (1004) o con el segundo dispositivo de red (1006).

2. Método según la reivindicación 1, que comprende además proporcionar, mediante el servidor (1010), una respuesta a una solicitud de credenciales al dispositivo digital (1002), basándose en la selección, comprendiendo la respuesta a la solicitud de credenciales las credenciales necesarias para acceder al primer dispositivo de red (1004) o al segundo dispositivo de red (1006) mediante el dispositivo digital (1002).

3. Método según la reivindicación 2, en el que el identificador de selección de red comprende una lista que incluye el primer identificador de dispositivo de red y el segundo identificador de dispositivo de red ordenados basándose en el análisis de atributo del primer atributo y del segundo atributo.

4. Método según la reivindicación 1, que comprende además comparar (1106), mediante el servidor (1010), el primer atributo y el segundo atributo con requisitos mínimos, en el que la selección, mediante el servidor (1010), del primer identificador de dispositivo de red o del segundo identificador de dispositivo de red también se basa al menos en parte en la comparación de los atributos con los requisitos mínimos.

5. Método según la reivindicación 1, que comprende además comparar (1112), mediante el servidor (1010), el primer atributo y el segundo atributo con una configuración personalizada, en el que la selección, mediante el servidor (1010), del primer identificador de dispositivo de red o del segundo identificador de dispositivo de red también se basa al menos en parte en la comparación de los atributos con la configuración personalizada.

6. Método según la reivindicación 1, que comprende además recibir (1110), mediante el servidor (1010), un identificador de usuario y recuperar la configuración personalizada a partir de una cuenta de usuario basándose en el identificador de usuario, y en el que los atributos comprenden una medición de rendimiento, un indicador de compartido y un identificador de servicio.

7. Sistema que comprende:

un dispositivo digital (1002) conectado a una red de comunicación y configurado para transmitir un primer identificador de dispositivo de red para un primer dispositivo de red (1004) que da acceso a una primera red, y un segundo identificador de dispositivo de red para un segundo dispositivo de red (1006) que da acceso a una segunda red por la red de comunicación; y

un servidor (1010) conectado a la red de comunicación y configurado para recibir el primer identificador de dispositivo de red para el primer dispositivo de red (1004) y el segundo identificador de dispositivo de red para el segundo dispositivo de red (1006) procedentes del dispositivo digital (1002), para obtener un primer perfil de red que comprende un primer atributo, basándose el primer perfil de red en el primer identificador de dispositivo de red, para obtener un segundo perfil de red que comprende un segundo atributo, basándose el segundo perfil de red en el segundo identificador de dispositivo de red, para seleccionar o el primer identificador de dispositivo de red o el segundo identificador de dispositivo de red basándose en un análisis de atributo del primer atributo y del segundo atributo, estando el identificador de dispositivo de red seleccionado asociado al primer o al segundo dispositivo de red con el fin de permitir al dispositivo digital seleccionar el primer o el segundo dispositivo de red para acceder a la

primera o a la segunda red basándose en la selección, y para proporcionar un identificador de selección de red inalámbrica, basándose en la selección, al dispositivo digital (1002), estando el identificador de selección de red inalámbrica asociado al primer dispositivo de red (1004) o al segundo dispositivo de red (1006) para permitir al dispositivo digital (1002) iniciar un acceso con el primer dispositivo de red asociado (1004) o con el segundo dispositivo de red (1006).

8. Sistema según la reivindicación 7, en el que el primer perfil y el segundo perfil se obtienen de una base de datos de red (1012).

9. Sistema según la reivindicación 7, en el que el servidor (1010) está además configurado para proporcionar una respuesta a la solicitud de credenciales basándose en la selección, comprendiendo la respuesta a la solicitud de credenciales las credenciales necesarias para acceder al primer dispositivo de red (1004) o al segundo dispositivo de red (1006) mediante el dispositivo digital (1002).

10. Sistema según la reivindicación 9, en el que el identificador de selección de red comprende una lista que incluye el primer identificador de dispositivo de red y el segundo identificador de dispositivo de red ordenados basándose en el análisis de atributo del primer atributo y del segundo atributo.

11. Sistema según la reivindicación 7, en el que el servidor (1010) está además configurado para:

comparar el primer atributo y el segundo atributo con requisitos mínimos, en el que la selección del primer identificador de dispositivo de red o del segundo identificador de dispositivo de red también se basa al menos en parte en la comparación de los atributos con los requisitos mínimos; o

comparar el primer atributo y el segundo atributo con la configuración personalizada, en el que la selección del primer identificador de dispositivo de red o del segundo identificador de dispositivo de red también se basa al menos en parte en la comparación de los atributos con la configuración personalizada.

12. Sistema según la reivindicación 11, en el que el servidor (1010) está además configurado para comparar la recepción de un identificador de usuario y la recuperación de la configuración personalizada a partir de una cuenta de usuario basándose en el identificador de usuario.

13. Sistema según la reivindicación 11, en el que los atributos comprenden una medición de rendimiento, un indicador de compartido y un identificador de servicio.

14. Un soporte legible por ordenador que transporta un código legible por ordenador para controlar un ordenador con el fin de llevar a cabo el método de cualquiera de las reivindicaciones de la 1 a la 6.

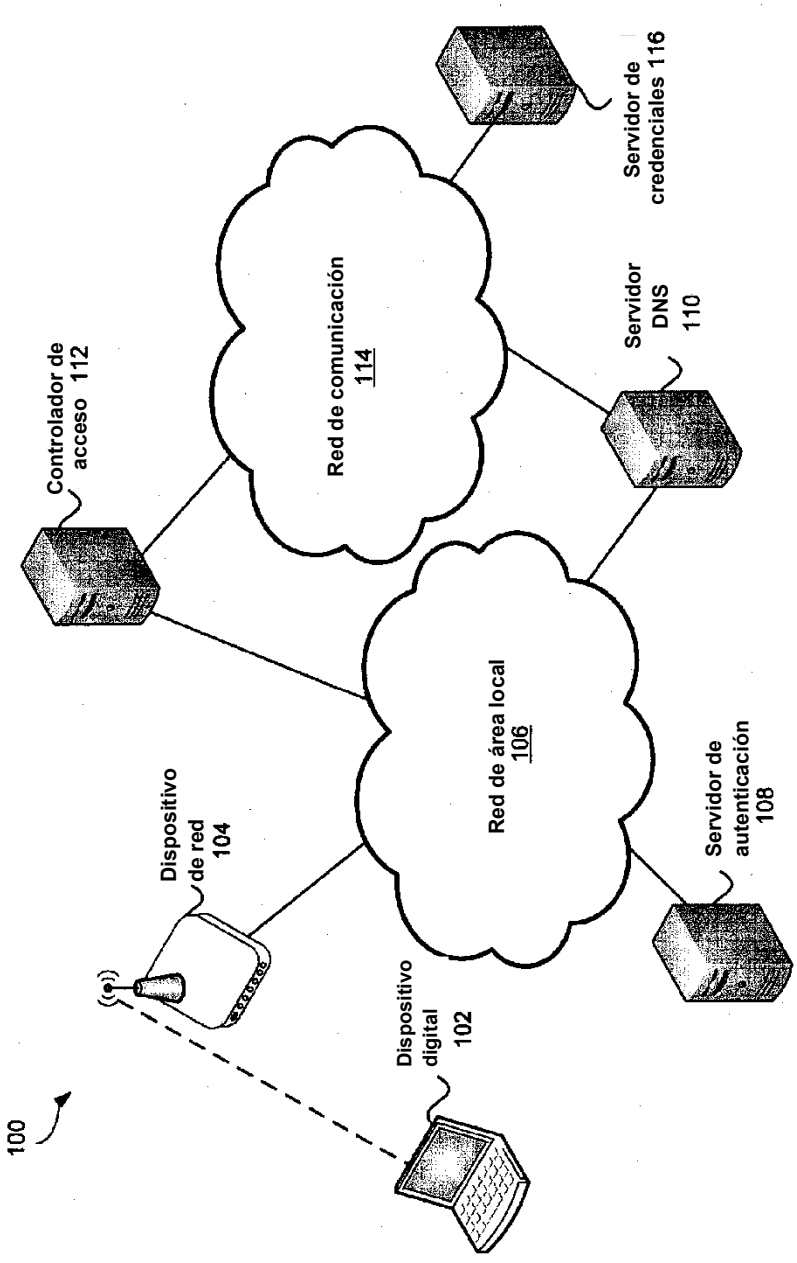
Servidor de credenciales 116
Red de comunicación 114
Servidor DNS 110
Controlador de acceso 112
Red de área local 106
Dispositivo de red 104
Servidor de autenticación 108
Dispositivo digital 102
100

FIG. 1

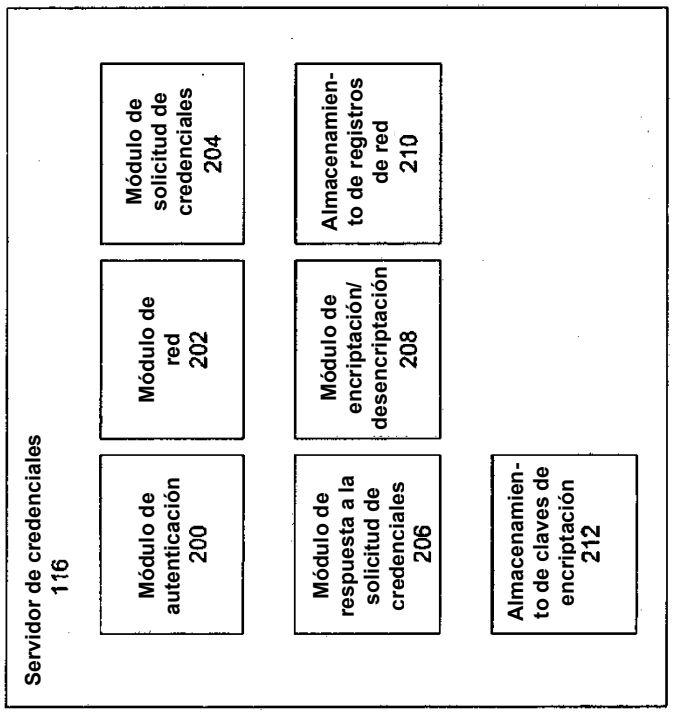
Servidor de credenciales
116
Módulo de autenticación
200
Módulo de red
202
Módulo de solicitud de credenciales
204
Módulo de respuesta a la solicitud de credenciales
206
Módulo de encriptación/ desencriptación
208
Almacenamiento de registros de red
210
Almacenamiento de claves de encriptación
212

FIG. 2

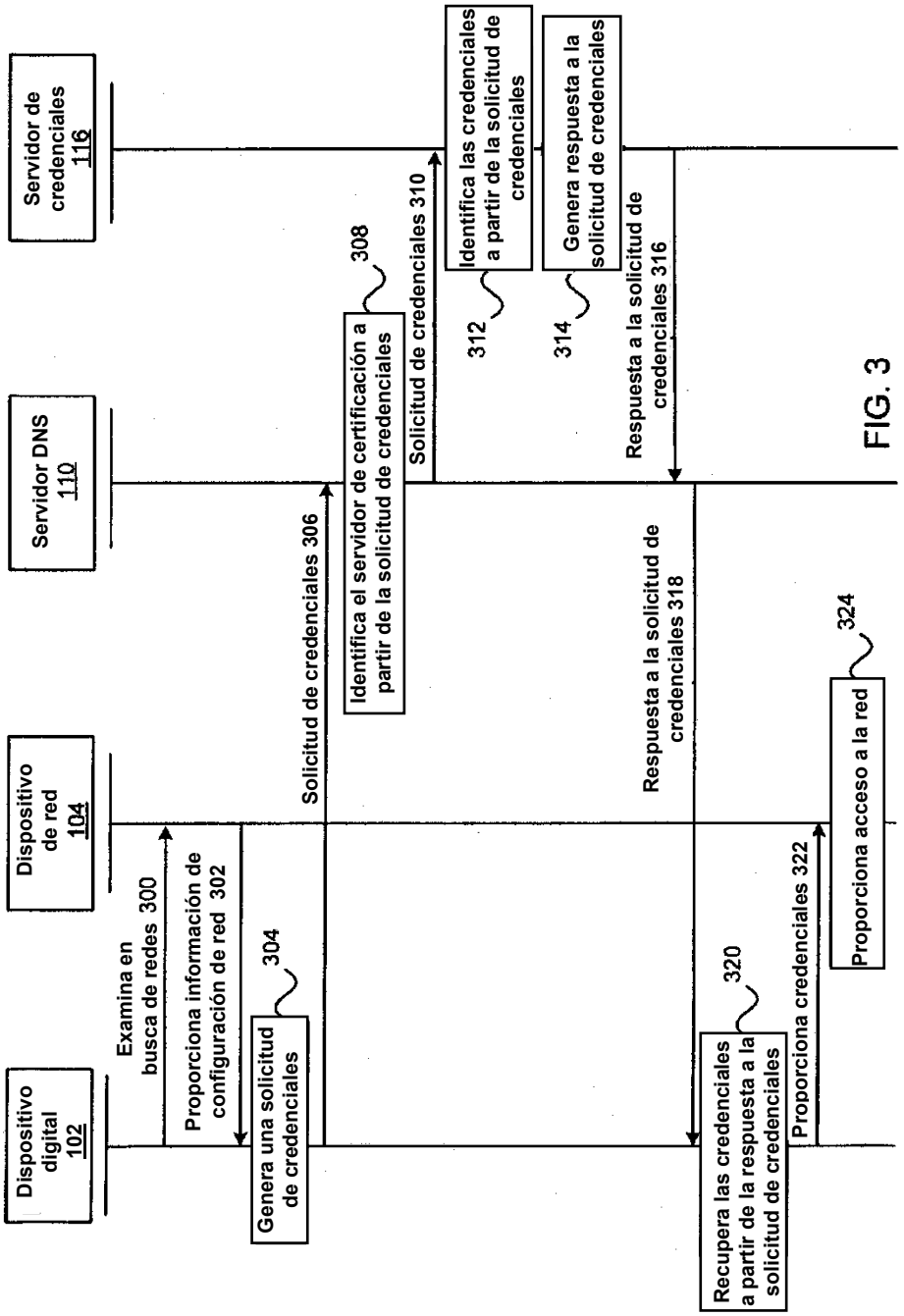
Dispositivo digital 102
Dispositivo de red 104
Servidor DNS 110
Servidor de credenciales 116
Examina en busca de redes 300
Proporciona información de configuración de red 302
Genera una solicitud de credenciales
304
Solicitud de credenciales 306
Identifica el servidor de certificación a partir de la solicitud de credenciales
308
Solicitud de credenciales 310
Identifica las credenciales a partir de la solicitud de credenciales
312
Genera respuesta a la solicitud de credenciales
314
Respuesta a la solicitud de credenciales 316
Respuesta a la solicitud de credenciales 318
Recupera las credenciales a partir de la respuesta a la solicitud de credenciales
320
Proporciona credenciales 322
Proporciona acceso a la red
324

FIG. 3

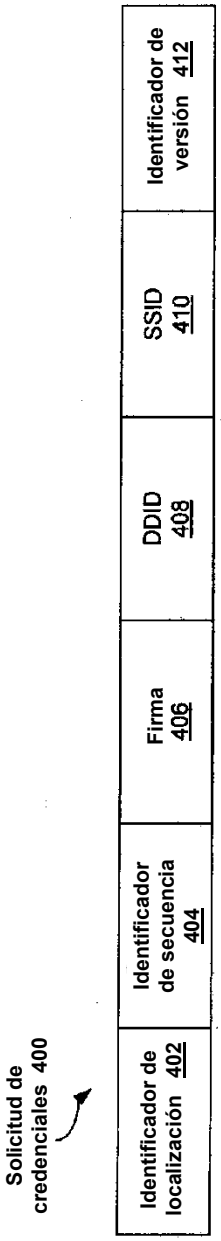
Solicitud de credenciales 400
Identificador de localización 402
Identificador de secuencia 404
Firma 406
DDID 408
SSID 410
Identificador de versión 412

FIG. 4

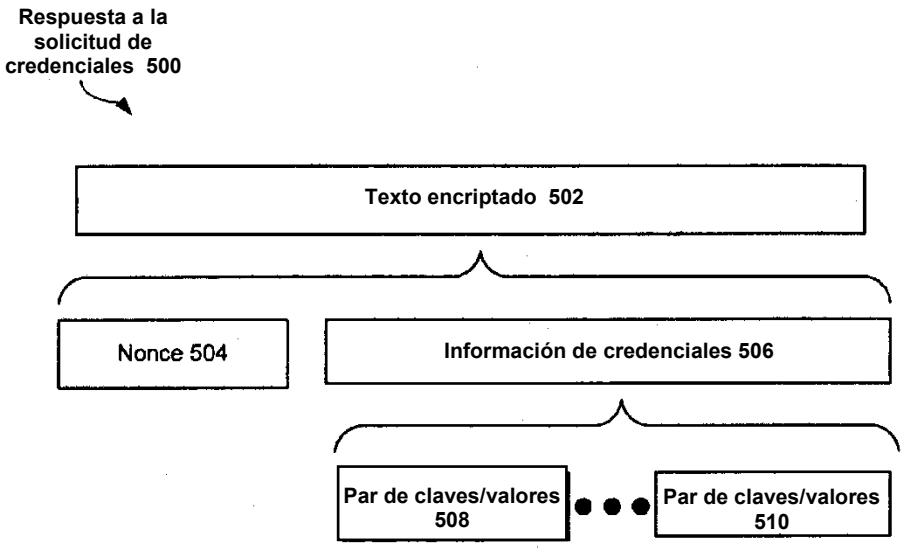
Respuesta a la solicitud de credenciales 500
Texto encriptado 502
Nonce 504
Información de credenciales 506
Par de claves/valores 508
Par de claves/valores 510

FIG. 5

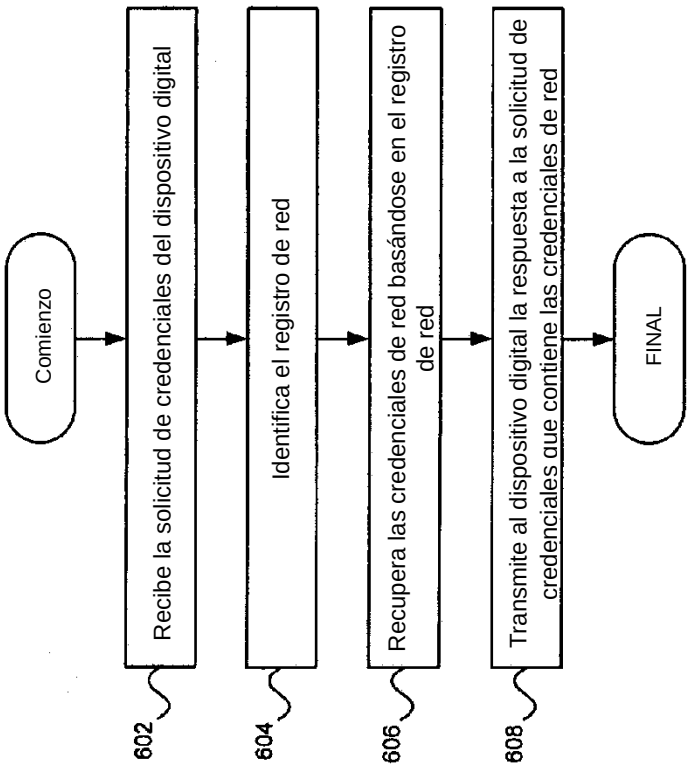
Comienzo
Recibe la solicitud de credenciales del dispositivo digital
Identifica el registro de red
Recupera las credenciales de red basándose en el registro de red
Transmite al dispositivo digital la respuesta a la solicitud de credenciales que contiene las credenciales de red
FINAL
602
604
606
608

FIG. 6

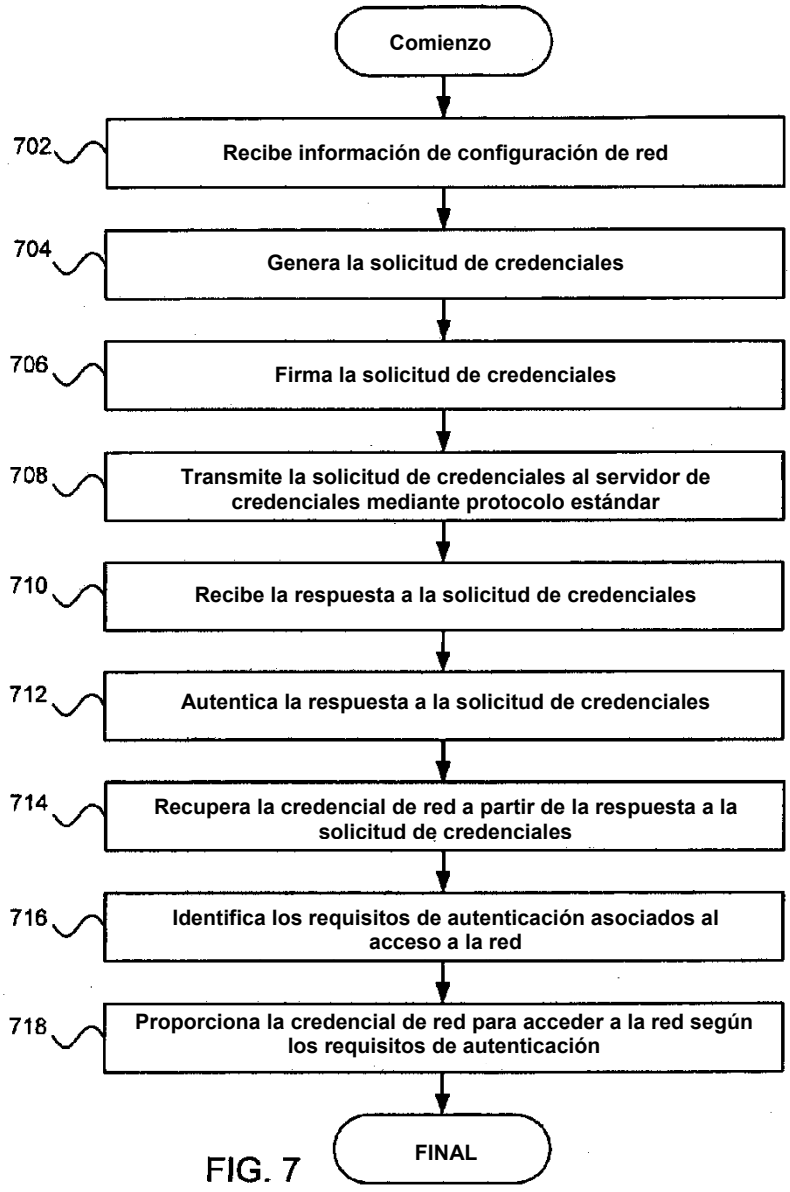
Comienzo
702
Recibe información de configuración de red
704
Genera la solicitud de credenciales
706
Firma la solicitud de credenciales
708
Transmite la solicitud de credenciales al servidor de credenciales mediante protocolo estándar
710
Recibe la respuesta a la solicitud de credenciales
712
Autentica la respuesta a la solicitud de credenciales
714
Recupera la credencial de red a partir de la respuesta a la solicitud de credenciales
716
Identifica los requisitos de autenticación asociados al acceso a la red
718
Proporciona la credencial de red para acceder a la red según los requisitos de autenticación
FINAL

FIG. 7

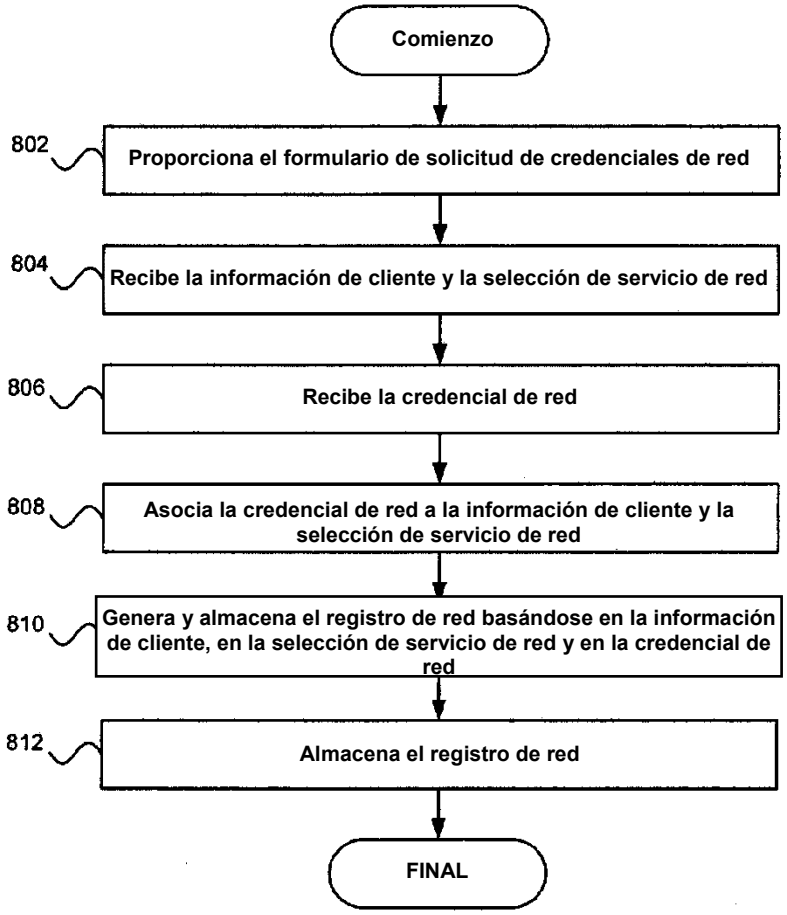
Comienzo
802
Proporciona el formulario de solicitud de credenciales de red
804
Recibe la información de cliente y la selección de servicio de red
806
Recibe la credencial de red
808
Asocia la credencial de red a la información de cliente y la selección de servicio de red
810
Genera y almacena el registro de red basándose en la información de cliente, en la selección de servicio de red y en la credencial de red
812
Almacena el registro de red
FINAL

FIG. 8

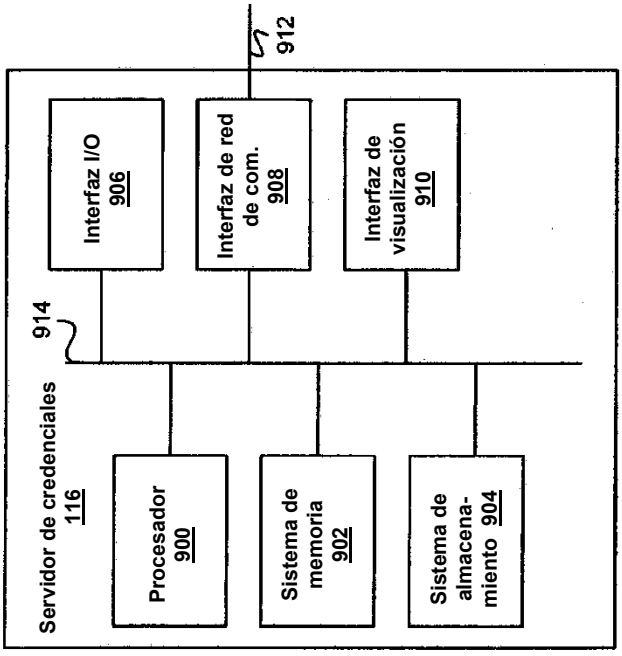
912
Interfaz I/O 906
Interfaz de red de com. 908
Interfaz de visualización 910
914
Servidor de credenciales 116
Procesador 900
Sistema de memoria 902
Sistema de almacena-miento 904

FIG. 9

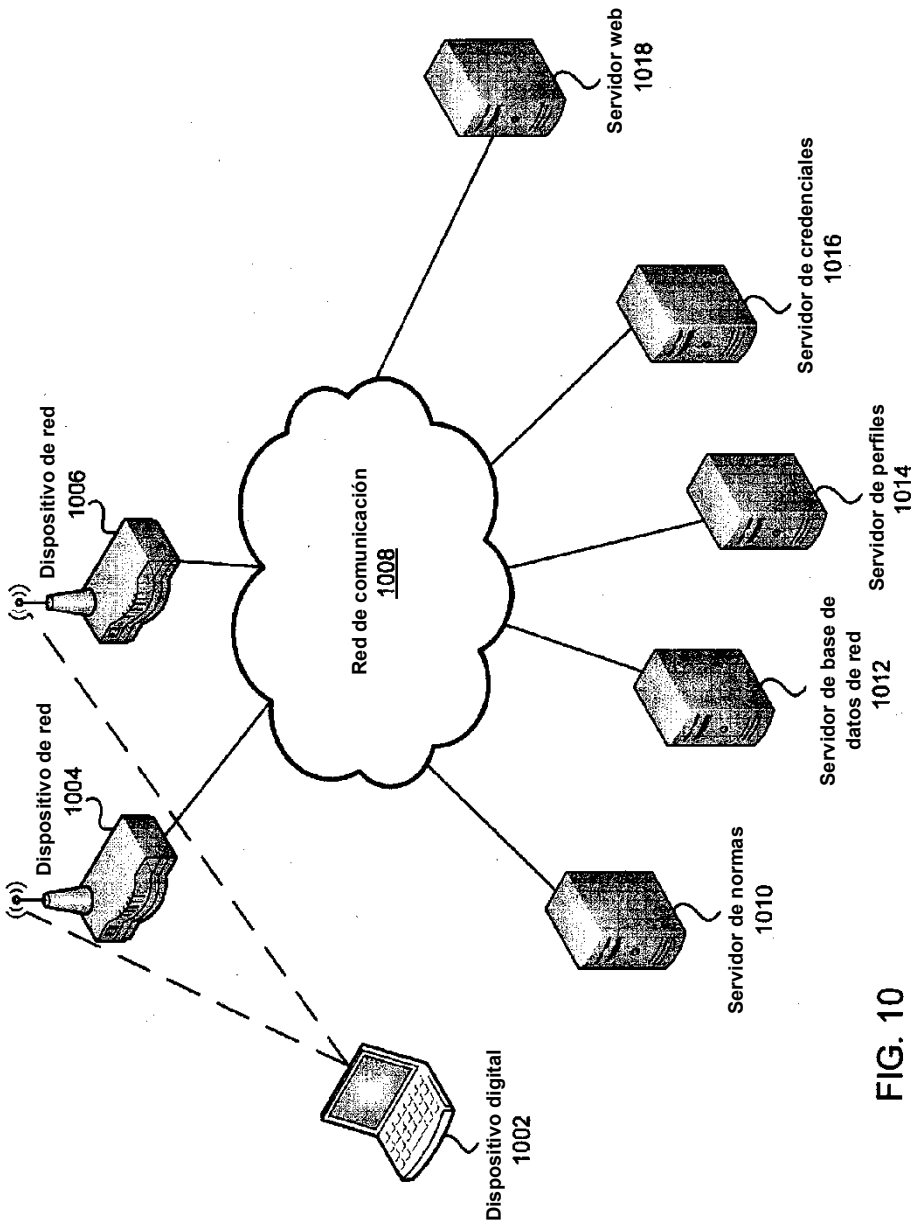
Servidor web
1018
Servidor de credenciales
1016
Servidor de perfiles
1014
Servidor de base de datos de red
1012
Servidor de normas
1010
Red de comunicación
1008
Dispositivo de red
1006
Dispositivo de red
1004
Dispositivo digital
1002

FIG. 10

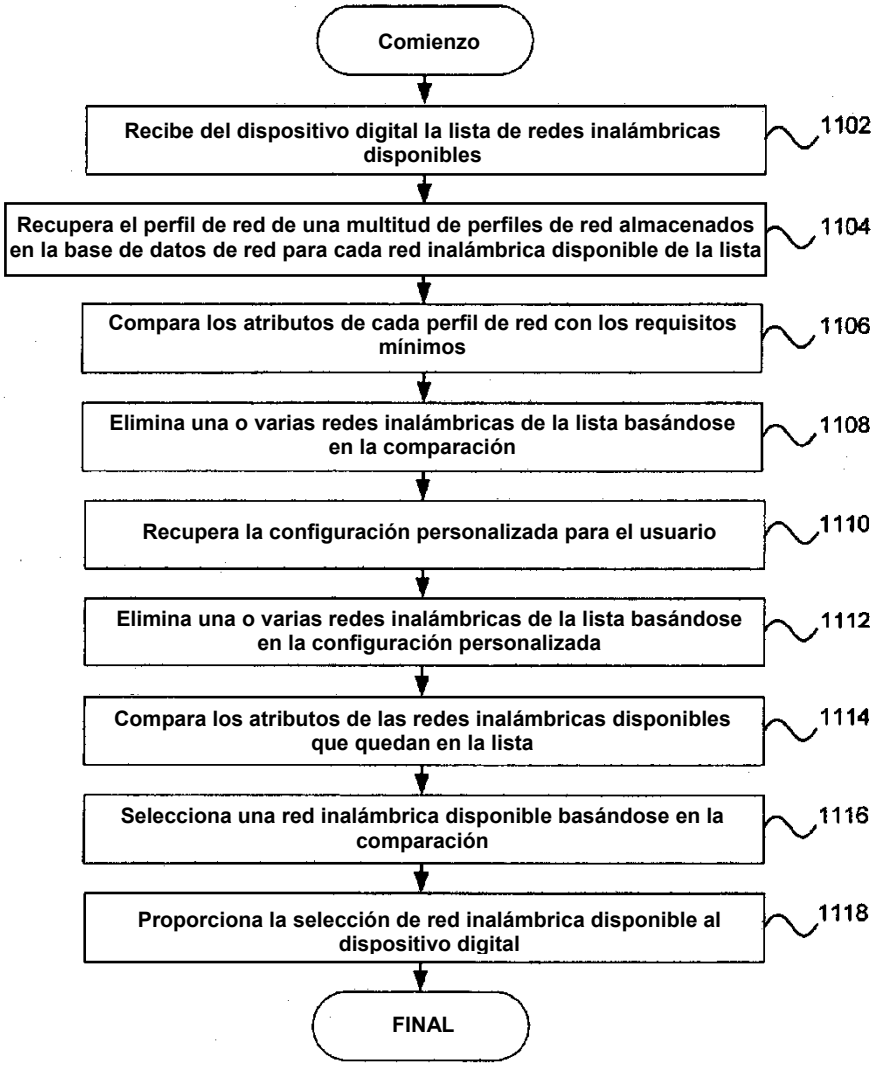
Comienzo
Recibe del dispositivo digital la lista de redes inalámbricas disponibles
1102
Recupera el perfil de red de una multitud de perfiles de red almacenados en la base de datos de red para cada red inalámbrica disponible de la lista
1104
Compara los atributos de cada perfil de red con los requisitos mínimos
1106
Elimina una o varias redes inalámbricas de la lista basándose en la comparación
1108
Recupera la configuración personalizada para el usuario
1110
Elimina una o varias redes inalámbricas de la lista basándose en la configuración personalizada
1112
Compara los atributos de las redes inalámbricas disponibles que quedan en la lista
1114
Selecciona una red inalámbrica disponible basándose en la comparación
1116
Proporciona la selección de red inalámbrica disponible al dispositivo digital
1118
FINAL

FIG. 11

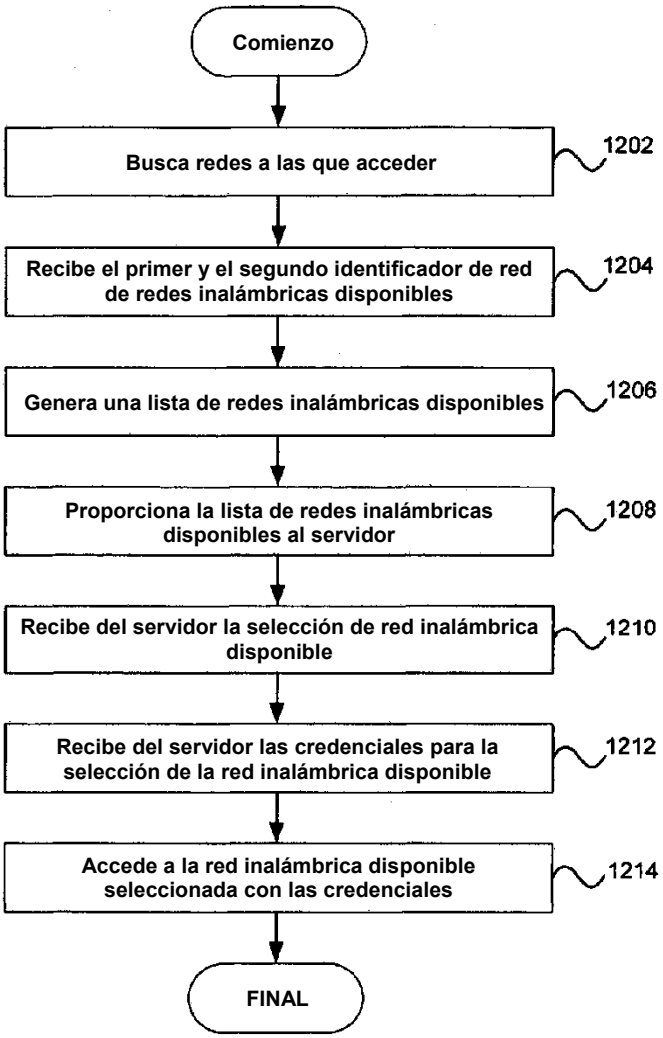
Comienzo
Busca redes a las que acceder
1202
Recibe el primer y el segundo identificador de red de redes inalámbricas disponibles
1204
Genera una lista de redes inalámbricas disponibles
1206
Proporciona la lista de redes inalámbricas disponibles al servidor
1208
Recibe del servidor la selección de red inalámbrica disponible
1210
Recibe del servidor las credenciales para la selección de la red inalámbrica disponible
1212
Accede a la red inalámbrica disponible seleccionada con las credenciales
1214
FINAL

FIG. 12

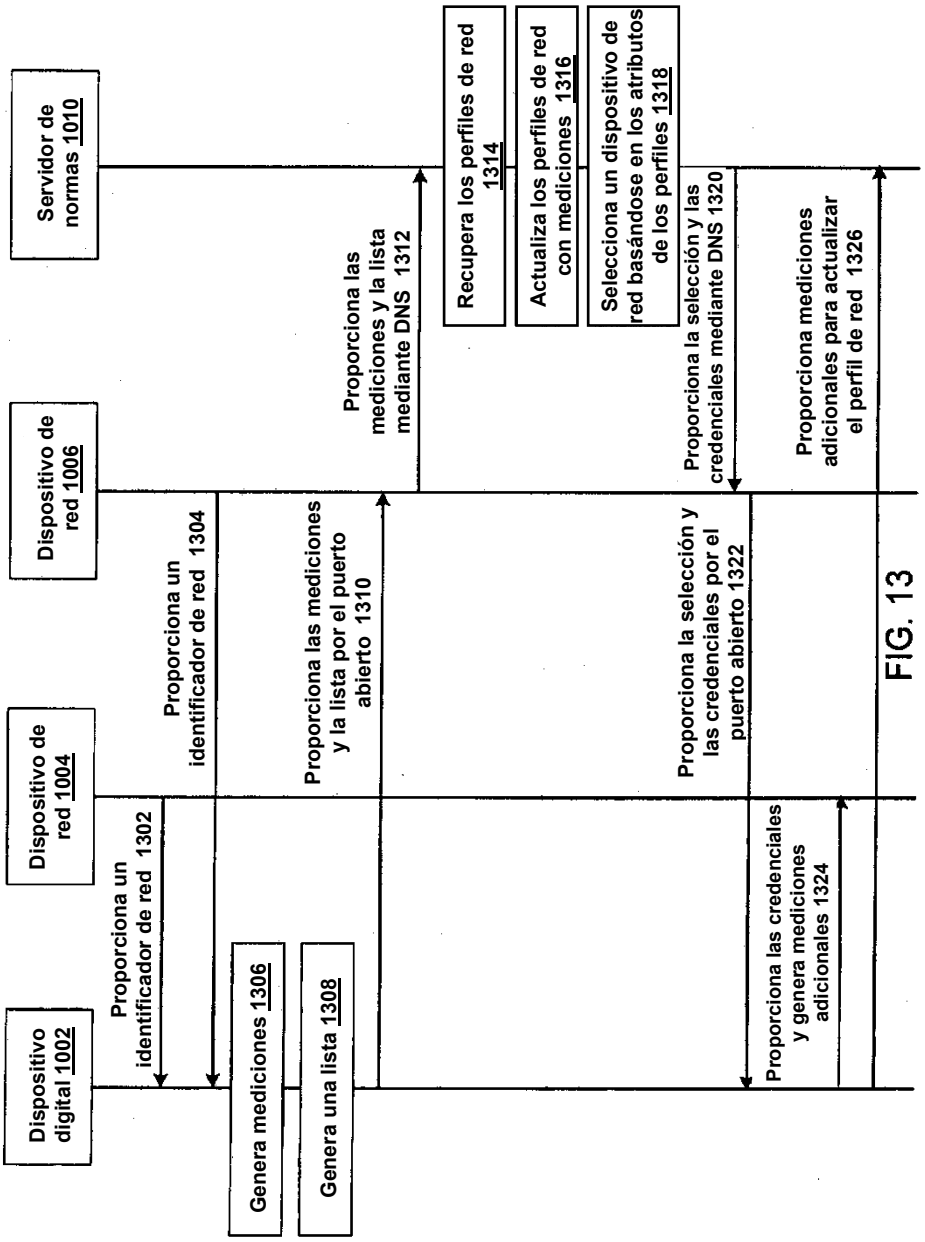
Dispositivo digital 1002
Dispositivo de red 1004
Dispositivo de red 1006
Servidor de normas 1010
Proporciona un identificador de red 1302
Proporciona un identificador de red 1304
Genera mediciones 1306
Genera una lista 1308
Proporciona las mediciones y la lista por el puerto abierto 1310
Proporciona las mediciones y la lista mediante DNS 1312
Recupera los perfiles de red 1314
Actualiza los perfiles de red con mediciones 1316
Selecciona un dispositivo de red basándose en los atributos de los perfiles 1318
Proporciona la selección y las credenciales mediante DNS 1320
Proporciona la selección y las credenciales por el puerto abierto 1322
Proporciona las credenciales y genera mediciones adicionales 1324
Proporciona mediciones adicionales para actualizar el perfil de red 1326

FIG. 13