(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 832 848**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 48/14 (2009.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.04.2010 E 18162627 (6)**

(97) Fecha y número de publicación de la concesión europea: **26.08.2020 EP 3364628**

(54) Título: **Método y aparato para descubrir información de autentificación en un entorno de red inalámbrica**

(30) Prioridad:

24.04.2009 US 172597 P
16.07.2009 US 504500

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.06.2021

(73) Titular/es:

BLACKBERRY LIMITED (100.0%)
2200 University Avenue East
Waterloo, Ontario N2K 0A7, CA

(72) Inventor/es:

MCCANN, STEPHEN y
MONTEMURRO, MICHAEL

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

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

DESCRIPCIÓN

Método y aparato para descubrir información de autentificación en un entorno de red inalámbrica

Solicitudes relacionadas

Campo de la divulgación

La presente divulgación se relaciona en general con comunicaciones de red y, más en particular, con métodos y aparato para descubrir información de autentificación en un entorno de red inalámbrica.

Antecedentes

Los despliegues de redes inalámbricas, tales como redes de área local inalámbricas (WLANs), permiten que los terminales inalámbricos accedan a la red y a servicios de Internet cuando están dentro de la proximidad de señales de comunicación inalámbrica de esas redes inalámbricas. Las WLANs disponibles comercialmente, tales como las ubicadas en entornos minoristas u otros establecimientos de acceso público, operan en modos no seguros para habilitar que los terminales inalámbricos establezcan comunicaciones con las WLANs y redes externas (por ejemplo, redes de proveedores de servicios, redes de operadores, etc.) accesibles a través de esas WLANs. Este modo no seguro de operación permite que los terminales inalámbricos negocien información de conexión y registro con las redes externas a través de comunicaciones de alto nivel usando direcciones de protocolo de Internet (IP) y un protocolo de transferencia de hipertexto (HTTP) para habilitar el registro de los terminales inalámbricos con las redes externas. Sin embargo, tales modos no seguros de operación que usan comunicaciones de alto nivel dejan las redes externas vulnerables a ataques maliciosos u otras actividades indeseables dirigidas a eludir procedimientos de red creados para el registro de terminal inalámbrico ordenado y determinista.

ARKKO J. et al en "Network Discovery and Selection Problem; rfc5113.txt", enero de 2008, considera los problemas de selección de credenciales y cómo un usuario puede identificar redes de acceso con las cuales puede autentificarse con éxito antes de elegir un punto de conexión.

El "Draft Amendment to Standard Information Tec - Telecommunications and information exchange between systems-Local and Metropolitan networks-specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 7: Interworking with External Networks", IEEE UNAPPROVED DRAFT STD P802.11U/D3.0, mayo de 2008 (2008-05), páginas i-xvii, 1-166, divulga el uso de Servicio de Anuncio Genérico (GAS) por la red para informar a un terminal inalámbrico de tipos de autentificación (tales como términos y condiciones de aceptación o inscripción en línea).

Breve descripción de los dibujos

La figura 1 representa una red de comunicación de ejemplo en la cual una pluralidad de ubicaciones de acceso a red de área local inalámbrica están acopladas de manera comunicativa a una o más redes.

La figura 2 representa una arquitectura de capa de comunicación de ejemplo.

La figura 3 representa una estructura de datos de parámetros de autentificación (AuPs) de ejemplo.

La figura 4 representa una estructura de datos de capacidades de conjunto de servicios básicos (BSS) de ejemplo que puede ser usada en relación con el proceso de intercambio de mensajería de ejemplo de la figura 6 para descubrir información de autentificación en una red inalámbrica.

La figura 5 representa una estructura de datos de información de autentificación de ejemplo que puede ser usada en relación con el proceso de intercambio de mensajería de ejemplo de la figura 6 para descubrir información de autentificación en una red inalámbrica.

La figura 6 representa un proceso de intercambio de mensajería de ejemplo que puede ser usado para descubrir información de autentificación en una red inalámbrica.

La figura 7 representa otra estructura de datos de capacidades de conjunto de servicios básicos (BSS) de ejemplo que puede ser usada en relación con el proceso de intercambio de mensajería de ejemplo de la figura 9 para descubrir información de autentificación en una red inalámbrica.

La figura 8 representa otra estructura de datos de información de autentificación de ejemplo que puede ser usada en relación con el proceso de intercambio de mensajería de ejemplo de la figura 9 para descubrir información de autentificación en una red inalámbrica.

La figura 9 representa otro proceso de intercambio de mensajería de ejemplo que puede ser usado para descubrir información de autentificación en una red inalámbrica.

La figura 10 representa un terminal inalámbrico de ejemplo que puede ser usado para implementar los métodos y aparato de ejemplo descritos en este documento.

La figura 11 representa un punto de acceso inalámbrico de ejemplo que puede ser usado para implementar los métodos y aparato de ejemplo descritos en este documento.

La figura 12 representa un diagrama de flujo de ejemplo representativo de instrucciones legibles por ordenador que pueden ser usadas para descubrir información de autentificación en una red inalámbrica.

Descripción detallada

Aunque lo siguiente divulga métodos y aparato de ejemplo que incluyen, entre otros componentes, software ejecutado en hardware, debe anotarse que tales métodos y aparato son simplemente ilustrativos y no deben considerarse como limitantes. Por ejemplo, se contempla que cualquiera o todos estos componentes de hardware y software podrían ser incorporados exclusivamente en hardware, exclusivamente en software, exclusivamente en firmware, o en cualquier combinación de hardware, software, y/o firmware. Por consiguiente, aunque lo siguiente describe métodos y aparato de ejemplo, las personas que tienen experiencia normal en la técnica apreciarán fácilmente que los ejemplos proporcionados no son la única forma de implementar tales métodos y aparato.

Los métodos y aparato de ejemplo descritos en este documento pueden ser usados por un terminal inalámbrico para descubrir información de autentificación (AI) y parámetros de autentificación (AuP) requeridos para autentificar el terminal inalámbrico para la conexión a una red inalámbrica. Los métodos y aparato de ejemplo descritos en este documento pueden ser usados en relación con dispositivos de comunicación móviles, dispositivos informáticos móviles, o cualquier otro dispositivo capaz de comunicarse de manera inalámbrica con una red inalámbrica. Tales dispositivos, también denominados como terminales, terminales inalámbricos, o equipo de usuario (UE), pueden incluir teléfonos inteligentes móviles (por ejemplo, un teléfono inteligente BLACKBERRY®), asistentes digitales personales inalámbricos (PDA), ordenadores portables/portátiles/transportables con adaptadores inalámbricos, etc. Los métodos y aparato de ejemplo se describen en este documento en relación con el estándar de comunicación de red de área local inalámbrica (WLAN) conocido como IEEE® (Instituto de Ingenieros Eléctricos y Electrónicos) 802.11, el cual, entre otras cosas, define el interfuncionamiento con redes externas. Sin embargo, los métodos y aparato de ejemplo pueden ser implementados adicional o alternativamente en relación con otros estándares de comunicación inalámbrica incluyendo otros estándares de WLAN, estándares de red de área personal (PAN), estándares de red de área amplia (WAN), o estándares de comunicación celular.

Aunque los métodos y aparato de ejemplo descritos en este documento pueden ser implementados en cualquier entorno que proporcione acceso a WLAN para conectividad de red, los métodos y aparato de ejemplo pueden ser implementados de manera ventajosa en ubicaciones o entornos de acceso a WLAN en los cuales se espera que uno o más usuarios que portan respectivos terminales inalámbricos se conectarán y desconectarán frecuentemente de una WLAN a medida que ingresan y salen de las ubicaciones o entornos de acceso a WLAN. Las ubicaciones o entornos de WLAN a veces se conocen como "puntos de conexión" en referencia a una ubicación o entorno que está dentro del alcance de comunicación de señales de WLAN. Tales ubicaciones o entornos de WLAN de ejemplo incluyen cafeterías, tiendas minoristas, instalaciones educativas, entornos de oficina, aeropuertos, estaciones y vehículos de transporte público, hoteles, etc.

La experiencia de usuario asociada con técnicas o estándares conocidos para conectar un terminal inalámbrico a un punto de acceso (AP) de un punto de conexión a WLAN a menudo puede resultar frustrante. Por ejemplo, a menudo es necesario descubrir correctamente el identificador de red de radio (por ejemplo, un parámetro de Identificador de Conjunto de Servicios (SSID) IEEE® 802.11), y también puede ser necesario descubrir AI y AuPs particulares (elegidos por el propietario/proveedor de punto de conexión) necesarios para conectarse a la red soportada con WLAN (por ejemplo, una red externa) detrás del AP del punto de conexión.

En algunos casos, puede ser suficiente que un terminal inalámbrico proporcione un Identificador de Dirección de Red (NAI) que indique la identidad del usuario al AP para que proceda la autentificación y coloque el terminal inalámbrico en comunicación con la red externa detrás del AP. En otros casos, un terminal inalámbrico puede tener que estar provisto de, por ejemplo, una tarjeta de módulo de identidad de suscriptor (SIM) para que proceda la autentificación. Tales situaciones a menudo crean experiencias de usuario frustrantes cuando los terminales inalámbricos fallan en conectarse a ubicaciones de acceso a WLAN debido a la falta o carencia de información de autentificación. En otras situaciones, incluso cuando los usuarios conocen la información de autentificación particular que debe proporcionarse, el proceso de proporcionar tal información de autentificación desde el terminal inalámbrico al AP puede ser pesado (por ejemplo, entrada manual).

Con referencia particularmente a las ubicaciones de acceso a WLAN (o puntos de conexión a WLAN) que operan bajo el estándar de comunicación inalámbrica IEEE® 802.11, este estándar está actualmente careciendo de provisiones para proporcionar a los terminales inalámbricos los detalles necesarios relacionados con autentificación sobre redes soportadas con WLAN (por ejemplo, redes externas) a las cuales están conectados APs de WLAN. Así, un usuario que desea acceder a la red típicamente es requerido que configure manualmente algunos aspectos de un terminal inalámbrico compatible con IEEE® 802.11, a menos que el AP esté operando de una manera no segura abierta, en

cuyo caso, no se necesitan AuPs para acceder a la red. A medida que la tecnología de WLAN es desplegada además a lo largo de diferentes ubicaciones, el acceso no seguro abierto atraerá a cada vez menos proveedores de puntos de conexión a WLAN. Los métodos y aparato de ejemplo descritos en este documento pueden ser usados para habilitar que los terminales inalámbricos descubran u obtengan requisitos de AI y AuP asociados con puntos de conexión a WLAN, así, reduciendo sustancialmente o eliminando la dependencia de la participación de usuario al acceder a servicios inalámbricos, y de esa manera, mejorando las experiencias de usuario con tales servicios. A continuación, se describen escenarios de ejemplo en los cuales pueden ser usados ventajosamente los métodos y aparato de ejemplo en relación con la figura 1.

Aunque los métodos y aparato de ejemplo se describen en este documento en relación con habilitar que los terminales inalámbricos descubran los requisitos de AI y AuP de APs, los métodos y aparato de ejemplo también pueden ser usados para habilitar que los APs descubran los requisitos de AI y AuP de terminales inalámbricos. Por ejemplo, cuando un terminal inalámbrico ya está conectado a una red externa (por ejemplo, una red del proveedor de servicios inalámbricos a través de un enlace de datos celulares, una PAN a través de un enlace BLUETOOTH®, etc.), un AP puede estar configurado para descubrir requisitos de AI y AuP asociados con esa red externa al consultar el terminal inalámbrico usando las técnicas de ejemplo descritas en este documento. Los métodos y aparato de ejemplo descritos en este documento también pueden ser usados en relación con entornos de redes en malla para habilitar que un primer AP descubra los requisitos de AI y AuP asociados con un segundo AP al consultar un terminal inalámbrico que está conectado directamente al segundo AP o conectado indirectamente al segundo AP a través de uno u otros más terminales inalámbricos. De esta manera, el primer AP puede conectarse a una red externa asociada con el segundo AP si el primer AP tiene los valores requeridos de AI y/o AuP.

Pasando ahora a la figura 1, se muestra una red 100 de comunicación de ejemplo en la cual pueden ser implementados los métodos y aparato de ejemplo descritos en este documento. Como se muestra en la figura 1, la red 100 de comunicación de ejemplo incluye una pluralidad de ubicaciones 102a-c de acceso a WLAN que proporcionan acceso a una o más redes (por ejemplo, redes soportadas con WLAN o redes externas) a través de puntos 104a-c de acceso respectivos. En el ejemplo ilustrado, el punto de acceso (AP) 104a proporciona acceso a una red 106a privada, la cual a su vez proporciona acceso a una red de proveedor de servicios de suscripción A (SSPN-A) 108a. También en el ejemplo ilustrado, el AP 104b proporciona acceso a una red 106b privada, la cual a su vez proporciona acceso a una red de proveedor de servicios de suscripción B (SSPN-B) 108b. Las SSPNs 108a-b pueden ser propiedad y/u operadas por proveedores de servicios de suscripción de datos, proveedores de servicios de suscripción de Internet, proveedores de servicios de suscripción de medios (por ejemplo, audio/vídeo), proveedores de servicios de suscripción de comunicaciones inalámbricas, o cualquier combinación de los mismos.

El AP 104c proporciona acceso a una red 110 pública, la cual se muestra como proporcionando acceso al Internet 112. Aunque no se muestra, cada uno de los APs 104a-c está provisto con una estación de AP (es decir, una STA de AP), la cual es la interfaz o componente, tal como un adaptador de red o tarjeta de interfaz de red (NIC), que se conecta a un medio inalámbrico.

Cada una de las ubicaciones 102a-c de acceso a WLAN puede estar asociada con diferentes conjuntos de AuPs requeridos de un terminal 114 inalámbrico para obtener acceso a las redes 106a, 106b, y/o 110 a través de los APs 104a-c. Estos AuPs pueden ser seleccionados por los respectivos propietarios u operadores de las redes 106a, 106b y 110. Los AuPs pueden ser seleccionados con base en diferentes factores tales como, por ejemplo, niveles de seguridad deseados y/u objetivos comerciales. Por ejemplo, si la ubicación 102a de acceso a WLAN es un aeropuerto, la red 106a privada puede requerir relativamente más parámetros de autentificación de un terminal inalámbrico que requeriría un establecimiento minorista para minimizar o prevenir vulnerabilidades en las redes de ordenador de aeropuertos/aerolíneas. Adicional o alternativamente, las redes 106a-b privadas pueden tener diferentes términos de acuerdos contractuales con los respectivos proveedores de servicios de las SSPNs 108a-b, lo que lleva así a diferentes conjuntos de requisitos de AuP. Tales AuPs diferentes pueden estar relacionadas con diferentes estructuras de cobro/tarificación de acceso a red o diferentes acuerdos de itinerancia de dispositivos inalámbricos. Algunas redes, tal como la red 110 pública, pueden requerir menos AuPs o ninguno.

En cualquier caso, los métodos y aparato de ejemplo descritos en este documento pueden ser usados ventajosamente para habilitar que el terminal 114 inalámbrico se mueva entre diferentes ubicaciones de acceso a WLAN (por ejemplo, las ubicaciones 102a-c de acceso a WLAN) sin requerir que el terminal 114 inalámbrico esté preconfigurado o precargado con diferentes conjuntos o listas de requisitos de AuP asociados con el acceso a esas diferentes ubicaciones de acceso a WLAN. De esta manera, el terminal 114 inalámbrico puede recibir o aprender dinámicamente AuPs requeridos de cualquier AP que no haya encontrado antes o que haya tenido sus AuPs requeridos cambiados desde una sesión de acceso previa entre el terminal 114 inalámbrico y el AP. En los ejemplos ilustrados descritos en este documento, el terminal 114 inalámbrico incluye una estación sin AP (es decir, una STA sin AP), mientras que cada uno de los APs 104a-c incluye una STA de AP respectiva.

Como se muestra en general en relación con la ubicación 102a de acceso a WLAN, el terminal 114 inalámbrico puede recuperar la AI requerida (incluyendo AuPs) del AP 104a transmitiendo un mensaje 116 de solicitud de AI y recibiendo un mensaje 118 de respuesta de AI que incluye identificadores que indican uno o más AI y/o AuPs requeridos. En el ejemplo ilustrado, el mensaje 116 de solicitud de AI y el mensaje 118 de respuesta de AI pueden ser intercambiados antes de un proceso de autentificación usando un protocolo de consulta predefinido tal como un formato de

consulta/respuesta de Servicio de Anuncio Genérico (GAS). El formato de consulta de GAS, como se define en IEEE® 802.11, habilita que las STAs sin AP (por ejemplo, el terminal 114 inalámbrico) descubran la disponibilidad de información (por ejemplo, capacidades de AP, AI, AuPs, etc.) relacionada con los servicios de red deseados. Alternativamente, el mensaje 116 de solicitud de AI y el mensaje 118 de respuesta de AI pueden ser intercambiados durante un proceso de autentificación de acuerdo con, por ejemplo, provisiones en el estándar IEEE® 802.11 que involucran comunicaciones seguras de negociación que intercambian de manera segura información para asegurar la confidencialidad de tal información.

Pasando a la figura 2, se muestra una arquitectura 200 de capa de comunicación de ejemplo con siete capas que pueden ser implementadas de acuerdo con el bien conocido Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI). En el ejemplo ilustrado, la arquitectura 200 de capa de comunicación incluye una capa 202 de enlace de datos, la cual incluye una subcapa 204 de control de acceso al medio (MAC). Para habilitar que los terminales inalámbricos (por ejemplo, el terminal 114 inalámbrico de la figura 1) recuperen AI y AuPs de APs inalámbricos (por ejemplo, los APs 102a-c inalámbricos de la figura1), los métodos y aparato de ejemplo descritos en este documento pueden ser usados para realizar operaciones o procesos que incluyen mensajería 206 de AI (por ejemplo, el mensaje 116 de solicitud de AI y el mensaje 118 de respuesta de AI de la figura 1) en la subcapa 204 de MAC. Es decir un terminal inalámbrico puede recuperar valores de AI y/o valores de AuP requeridos de una memoria u otro hardware del terminal inalámbrico usando uno o más procesos de recuperación de valor de autentificación realizados por el terminal inalámbrico en la subcapa 204 de MAC sin necesidad de permitir que los procesos de recuperación de valor de autentificación realicen operaciones en o por encima de una capa de protocolo de internet (IP) (por ejemplo, una capa 208 de red) sin necesidad de proporcionar de otra manera los procesos de recuperación de valor de autentificación con acceso a la capa de IP.

Algunas técnicas de autentificación que usan el protocolo de transferencia de hipertexto (HTTP) u otros procesos de protocolo de internet (IP) para desplegar sitios web de inicio de sesión y/o sitios web de términos y condiciones requieren establecer una conexión entre un terminal inalámbrico y un AP inalámbrico en una o más de las capas entre e incluyendo una capa 208 de red (por ejemplo, una capa de protocolo de internet (IP)) y una capa 210 de aplicación de la arquitectura 200 de capa de comunicación. Sin embargo, tales técnicas a menudo pueden crear ciertas vulnerabilidades a las redes soportadas con WLAN (por ejemplo, una de las redes 106a-b privadas) que pueden ser explotadas de formas dañinas por usuarios maliciosos o dañinos. Es decir, usuarios pueden acceder a recursos de red usando técnicas de desviación de autentificación con base en comunicaciones de IP o HTTP u otros protocolos de comunicación en o por encima de la capa 208 de red. La mensajería 206 de AI usada en relación con los métodos y aparato de ejemplo descritos en este documento puede reducir sustancialmente o eliminar tales vulnerabilidades usando un proceso de autentificación que involucra operaciones en una conexión de red de subcapa de MAC haciéndolo relativamente más difícil o imposible para los usuarios acceder a tales recursos de red de bajo nivel para desviar los procesos de autentificación.

Además, las técnicas de autentificación implementadas en o por encima de la capa 208 de red requieren relativamente más potencia de procesamiento de un terminal inalámbrico que implementar procesos en la subcapa 204 de MAC. Terminales inalámbricos móviles (por ejemplo, el terminal 114 inalámbrico de la figura 1) tales como teléfonos inteligentes móviles, PDAs, etc. a menudo tienen ciclos de procesador relativamente limitados y potencia eléctrica disponible que los dispositivos informáticos de ubicación fija alimentados usando fuentes de electricidad de corriente alterna (AC). Así, los métodos y aparato de ejemplo descritos en este documento pueden ser usados ventajosamente para configurar, diseñar, o construir de otro modo terminales inalámbricos móviles para que operen de manera más eficiente (es decir, hacer más con menos ciclos de procesador) mientras que se minimiza el uso de potencia de batería. Es decir, los métodos y aparato de ejemplo descritos en este documento pueden ser usados ventajosamente para promover diseños de terminales inalámbricos móviles que consumen relativamente menos consumo de potencia y operan de manera relativamente más eficiente. Por ejemplo, las operaciones de recursos de bajo nivel en la subcapa 204 de MAC requieren relativamente menos recursos de sistema que las operaciones intensivas en interfaz de usuario e intensivas en sistema operativo (OS) (por ejemplo, operaciones de navegador web) en la capa 210 de aplicación.

Otra ventaja de ejemplo de la mensajería 206 de AI en la subcapa 204 de MAC es que un terminal inalámbrico puede, sin la participación de usuario o con participación mínima de usuario, determinar si la conexión a un AP particular es incluso una opción con base en la AI y/o AuPs requeridos anunciados por ese AP y que pueden ser solicitados por la red detrás del AP. Por ejemplo, si el AP 104a indica que requiere un identificador de tarjeta de SIM, y el terminal 114 inalámbrico no tiene una tarjeta de SIM que almacene un código particular, un usuario del terminal 114 inalámbrico no se le da la opción de descubrir que el AP está disponible para conexión. Así, durante un proceso de descubrimiento de WLAN iniciado por el usuario del terminal 114 inalámbrico, el terminal 114 inalámbrico no regresa el SSID del AP 104a debido a que no sería posible que el terminal 114 inalámbrico se conecte al AP 104a sin una tarjeta de SIM. Tal implementación reduciría sustancialmente o eliminaría la frustración de usuario debido a que el usuario no participaría en ningún intento de conectarse cuando tal conexión es imposible con base en las credenciales del usuario. En tal ejemplo, el requisito de tarjeta de SIM puede ser impuesto por un proveedor de servicios inalámbricos que posee u opera la SSPN-A 108a para, por ejemplo, asegurar que solo los terminales inalámbricos (por ejemplo, teléfonos inteligentes) asociados con su servicio puedan obtener acceso a red. Es decir, cuando el terminal 114 inalámbrico determina que tiene el requisito de tarjeta de SIM, despliega el SSID del AP104a debido a que puede ser autentificado por el AP 104a. Aunque es usado un SSID en relación con el ejemplo anterior y en otros ejemplos descritos a continuación, un AP puede estar configurado alternativamente para radiodifundir un Identificador de Conjunto de

Servicios Extendido Homogéneo (HESSID). Un HESSID incluye un SSID asociado con un AP particular y una identificación de red que corresponde a una SSPN soportada. Por ejemplo, si el AP 104a de la figura 1 fue configurado para radiodifundir un HESSID, incluiría el SSID del AP 104a y la identificación de red que corresponde a la SSPN-A 108a.

La figura 3 representa una estructura 300 de datos de parámetros de autentificación (AuPs) de ejemplo mostrada en formato de tabla para facilitar su descripción. La estructura 300 de datos de AuPs de ejemplo incluye una pluralidad de nombres 302 de AuP, cada uno de los cuales está asociado con uno respectivo de una pluralidad de identificadores 304 de AuP. En el ejemplo ilustrado, los identificadores 304 de AuP no son en sí mismos valores de AuP, sino que en vez son identificadores usados por los APs inalámbricos (por ejemplo, los APs 104a-c inalámbricos de la figura 1) para indicar a los terminales inalámbricos (por ejemplo, el terminal 114 inalámbrico de la figura 1) cuales valores de AuP deben tener los terminales inalámbricos para ser autentificados y establecer comunicaciones de red a través de los APs inalámbricos. Por ejemplo, de acuerdo con la estructura 300 de datos de AuPs, un NAI AuP ID (es decir, ID de AuP = 1) es usado para indicar al terminal 114 inalámbrico que el terminal 114 inalámbrico debe proporcionar un valor de AuP igual a una identidad del usuario asociada con el terminal 114 inalámbrico.

Los identificadores 304 de AuP identifican AuPs que típicamente involucran autentificación en la subcapa 204 de MAC. Sin embargo, en algunas implementaciones de ejemplo, algunos AuPs pueden involucrar solicitar una entrada de contraseña de usuario o una entrada de PIN. En el ejemplo ilustrado, la estructura 300 de datos de AuPs incluye un parámetro de indicador de dirección de red (NAI) (por ejemplo, una identidad del usuario de terminal inalámbrico), un parámetro de asunto de servidor, un parámetro de red de área de almacenamiento de servidor (SAN), y entradas reservadas para parámetros específicos de vendedor. En otras implementaciones de ejemplo, la estructura 300 de datos de AuPs puede proporcionarse con menos, más, y/o diferentes AuPs.

Los propietarios u operadores de redes soportadas con WLAN pueden seleccionar uno o más de los AuPs en la estructura 300 de datos de AuPs como AuPs requeridos para permitir la autentificación y conexión a sus redes soportadas con WLAN. En algunas implementaciones de ejemplo, el terminal 114 inalámbrico puede estar configurado para almacenar una lista completa de los AuPs en la estructura 300 de datos de AuPs, mientras que, en otras implementaciones de ejemplo, el terminal 114 inalámbrico puede estar configurado para almacenar los seleccionados de los AuPs. Por ejemplo, si el terminal 114 inalámbrico es proporcionado por un proveedor de servicios de telefonía móvil inalámbrica que elige permitir que sus dispositivos se conecten de manera inalámbrica solo a puntos de conexión a WLAN patrocinados o aprobados usando valores de identificación de tarjeta de SIM, el terminal 114 inalámbrico puede almacenar solo un identificador de AuP de NAI (ID de AuP = 1) asociado con la estructura 300 de datos de AuPs además de un identificador de hardware de seguridad discutido a continuación en relación con la figura 5. En tal implementación de ejemplo, el identificador de AuP de NAI se refiere a requerir un valor de identificación de usuario, y el identificador de hardware de seguridad se refiere a requerir un valor de identificación de tarjeta de SIM (u otro valor de identificación que corresponde a otro elemento de hardware de seguridad (por ejemplo, una tarjeta de SIM universal (USIM) o un elemento seguro de comunicación de campo cercano (NFC))).

El terminal 114 inalámbrico puede estar configurado para descubrir uno o más de los AuPs en la estructura 300 de datos de AuPs usando la técnica de descubrimiento de AI de ejemplo descrita a continuación en relación con las figuras 4-6, o usando la técnica de descubrimiento de AI de ejemplo descrita a continuación en relación con las figuras 7-9.

Como se discute a continuación en relación con las figuras 4-6, un AP puede estar configurado para anunciar sus requisitos de autentificación como dos tipos separados de capacidades de autentificación, el primero de los cuales involucra un terminal inalámbrico que realiza operaciones o procesos en o por encima de la capa 208 de red (figura 2) y el segundo de los cuales involucra el terminal inalámbrico que realiza operaciones en la subcapa 204 de MAC (o la capa 202 de enlace de datos) (figura 2). Operaciones en o por encima de la capa 208 de red (por ejemplo, operaciones de IP en la capa 208 de red, operaciones de HTTP en la capa 210 de aplicación, etc.) pueden incluir obtener una confirmación de que un usuario aceptó términos y condiciones particulares y/u obtener un nombre de usuario de inicio de sesión y/o credenciales de contraseña usando una página de inicio de sesión que se despliega con una operación de redireccionamiento de localizador de recursos uniforme (URL).

En implementaciones de ejemplo alternativas, como se discute a continuación en relación con las figuras 7-9, un AP puede estar configurado para anunciar una única capacidad de autentificación que puede indicar requisitos de autentificación que involucran operaciones en la subcapa 204 de MAC (o la capa 202 de enlace de datos) y requisitos de autentificación que involucran operaciones en o por encima de la capa 208 de red.

Pasando ahora a las figuras 4-6, la figura 4 representa una estructura 400 de datos de capacidades de conjunto de servicios básicos (BSS) de ejemplo, la figura 5 representa una estructura 500 de datos de información de autentificación (AI) de capa 2 de ejemplo, y la figura 6 representa un proceso de mensajería de ejemplo (por ejemplo, el cual puede ser usado para implementar la mensajería 206 de AI de la figura 2) para descubrir AI en un entorno de WLAN (por ejemplo, una de las ubicaciones 102a-c de acceso a WLAN de la figura 1). El proceso de mensajería de ejemplo de la figura 6 puede ser usado en relación con la información en la estructura 400 de datos de capacidades de BSS y la estructura 500 de datos de AI de capa 2 para implementar una técnica de descubrimiento de AI de ejemplo que involucra usar una primera consulta de AI para descubrir requisitos de AI asociados con operaciones en la subcapa

204 de MAC (figura 2) y una segunda consulta de AI para descubrir requisitos de AI asociados con operaciones en o por encima de la capa 208 de red (figura 2).

La estructura 400 de datos de capacidades de BSS de ejemplo almacena IDs 402 de CAP (es decir, identificadores de capacidad) de APs y/o terminales inalámbricos. En el ejemplo ilustrado, la estructura 400 de datos de capacidades de BSS incluye una entrada 404 de capacidad de información de tipo de autentificación de capa 3+ y una entrada 406 de capacidad de información de tipo de autentificación de capa 2, cada una asociada con uno respectivo de los IDs 402 de CAP. La entrada 404 de capacidad de información de tipo de autentificación de capa 3+ y la entrada 406 de capacidad de información de tipo de autentificación de capa 2 son usadas para indicar las capacidades de los APs 104a-c de la figura 1. Así, en el ejemplo ilustrado, la estructura 400 de datos de capacidades de BSS puede ser almacenada en los APs 104a-c y son descubribles usando formatos de protocolo de consulta predefinidos por terminales inalámbricos (por ejemplo, el terminal 114 inalámbrico) que intentan conectarse a respectivas redes soportadas con WLAN (por ejemplo, las redes 106a-b y 110 de la figura 1). Un formato de protocolo de consulta predefinido de ejemplo incluye el formato de consulta de GAS descrito anteriormente.

En el ejemplo ilustrado, la entrada 404 de capacidad de información de tipo de autentificación de capa 3+ puede ser usada para indicar que el AP asociado requiere una autentificación de nivel de HTTP. Tal autentificación puede ser implementada usando técnicas de redireccionamiento de URL que involucran redireccionar un navegador web del terminal inalámbrico a un URL particular que requiere que un usuario de terminal inalámbrico realice etapas adicionales requeridas para el acceso (por ejemplo, aceptar términos y condiciones, inscripción de inicio de sesión en línea, etc.). La entrada 406 de capacidad de información de tipo de autentificación de capa 2 puede ser usada para indicar que el AP asociado requiere uno o más de los AuPs mostrados en la estructura 300 de datos de AuPs de la figura 3 y/o AI descrita a continuación en relación con la figura 5.

La estructura 500 de datos de AI de capa 2 de ejemplo de la figura 5 almacena información de autentificación que es recuperada por el terminal 114 inalámbrico de un AP (por ejemplo, uno de los APs 104a-c de la figura 1). En el ejemplo ilustrado, la estructura 500 de datos de AI de capa 2 puede ser usada para indicar protocolos o información que un AP requiere para intercambiar información y realizar procesos de autentificación. Los tipos o protocolos de AI se muestran como tipos 502 de AI, y cada tipo de AI está identificado mediante un ID 504 de AI correspondiente.

En el ejemplo ilustrado, la estructura 500 de datos de AI de capa 2 almacena un tipo 506 de AI de método de Protocolo de Autentificación Extensible (EAP), el cual puede ser usado para indicar que un AP (por ejemplo, uno de los APs 104a-c de la figura1) soporta y/o requiere uno o más protocolos de autentificación. EAP es un tipo de protocolo que puede ser usado para realizar procesos de autentificación en redes inalámbricas y a veces es usado en relación con los bien conocidos estándares de Acceso Protegido a Wi-Fi (WPA). En operación, las comunicaciones de EAP pueden ser invocadas por cualquiera de los APs 104a-c de la figura 1 de acuerdo con el bien conocido estándar IEEE® 802.IX, el cual es parte de la arquitectura IEEE® 802.11. Los métodos de EAP conocidos incluyen EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA, y PEAP. Cada método de EAP puede ser identificado usando un valor de formato entero correspondiente asignado por un cuerpo de coordinación de recursos estándar de industria tal como la Autoridad de Números Asignados de Internet (IANA) (http://www.iana.org). Otros métodos de EAP también pueden incluir métodos específicos de vendedor.

La estructura 500 de datos de AI de capa 2 de ejemplo también almacena un tipo 508 de AI de modo de autentificación interna, un tipo 510 de AI de tipo certificado, un tipo 512 de AI de hardware de seguridad, un tipo 514 de AI de AuP, y tipos 516 de AI específico de vendedor. El tipo 508 de AI de modo de autentificación interna puede ser usado para indicar que un AP (por ejemplo, uno de los APs 104a-c de la figura 1) soporta y/o requiere protocolos de tunelización seguros para intercambiar de manera segura información entre el AP y un terminal inalámbrico. El tipo 510 de AI de tipo certificado puede ser usado para indicar que un AP (por ejemplo, uno de los APs 104a-c de la figura 1) soporta y/o requiere certificados de seguridad para intercambiar de manera segura información. El tipo 512 de AI de hardware de seguridad puede ser usado para indicar que un AP soporta y/o requiere que un terminal inalámbrico tenga una o más credenciales proporcionadas por o suministradas por un elemento de hardware asociado con el terminal inalámbrico. Los elementos de hardware enumerados en el ejemplo ilustrado de la figura 5 incluyen una tarjeta de SIM, una tarjeta de USIM, un elemento seguro de NFC, y una contraseña de hardware.

El tipo 514 de AI de AuP puede ser usado para indicar cuál de los AuPs en la estructura 300 de datos de AuPs de la figura 3 son requeridos por un AP (por ejemplo, uno de los APs 104a-c de la figura 1) para permitir que un terminal inalámbrico sea autentificado para establecer una conexión de red con el AP. El tipo 516 de AI específico de vendedor puede ser usado para definir tipos de AI adicionales o alternativos definidos por propietarios u operadores de redes soportadas con WLAN (por ejemplo, las redes 106a-b, 108a-b, y 110 de la figura 1). Formatos de marco de mensajería de ejemplo que pueden ser usados por un terminal inalámbrico para recuperar la AI de la estructura 500 de datos de AI de capa 2 se describen a continuación en relación con la figura 6.

Con referencia ahora a la figura 6, el ejemplo ilustrado muestra un proceso 600 de intercambio de mensajería que puede ser usado para descubrir los requisitos de AI en una red inalámbrica en relación con las estructuras de datos descritas anteriormente en relación con las figuras 3-5. Como se muestra, el proceso 600 de intercambio de mensajería involucra una pluralidad de intercambios de consulta/respuesta entre el terminal 114 inalámbrico y el AP 104a para descubrir AI soportada y/o requerida por el AP 104a para permitir que el terminal 114 inalámbrico establezca una

conexión de red con la red 106a privada soportada con WLAN y/o la SSPN-A 108a de la figura 1. En el ejemplo ilustrado, las capacidades del AP 104a incluyen soporte para información de tipo de autentificación de capa 3+ descrita anteriormente en relación con la entrada 404 de capacidad de información de tipo de autentificación de capa 3+ de la figura 4 e información de tipo de autentificación de capa 2 descrita anteriormente en relación con la entrada 406 de capacidad de información de tipo de autentificación de capa 2 de la figura 4.

Como se muestra en la figura 6, el terminal 114 inalámbrico y el AP 104a realizan un primer conjunto de intercambios de mensajes que involucran una primera consulta 602 de capacidades y una primera respuesta 604 de capacidades, que permiten al terminal 114 inalámbrico descubrir cuáles de los AI y AuPs de la estructura 500 de datos de AI y la estructura 300 de datos de AuPs son requeridos por el AP 104a para autentificar el terminal 114 inalámbrico. En el ejemplo ilustrado, el terminal 114 inalámbrico y el AP 104a también realizan un segundo conjunto de intercambios de mensajes que involucran una segunda consulta 606 de capacidades y una segunda respuesta 608 de capacidades, que permite que el terminal 114 inalámbrico descubra la información de tipo de autentificación de capa 3+ (por ejemplo, información de autentificación a nivel de IP, información de autentificación a nivel de HTTP, etc.) que es soportada y/o requerida por el AP 104a. Las consultas 602 y 606 pueden ser realizadas por el terminal 114 inalámbrico usando el formato de consulta de GAS descrito anteriormente. Aunque las consultas/respuestas 602/604 y 606/608 se describen como primera y segunda consulta/respuestas, tal descripción no implica ningún orden requerido de los conjuntos de intercambios de mensajes. Es decir, el intercambio de consulta/respuesta 606/608 podría ser realizado alternativamente antes del intercambio de consulta/respuesta 602/604. Además, cualquiera de los intercambios de consulta/respuesta 602/604 y 606/608 podría producirse sin el otro.

Para permitir que el terminal 114 inalámbrico descubra información de tipo de autentificación de capa 2, el AP 104a responde a la consulta 602 de capacidades comunicando un marco 610 de información de tipo de autentificación de capa 2 al terminal 114 inalámbrico a través de la respuesta 604 de capacidades. En el ejemplo ilustrado, el marco 610 de información de tipo de autentificación de capa 2 incluye un campo 612 de ID de CAP, un campo 614 de longitud, un campo 616 de conteo, y una pluralidad de campos de identificador de información de autentificación (ID de AI) y campos de valor de AI correspondientes.

El campo 612 de ID de CAP identifica la capacidad de BSS con la cual está asociado el marco 610. Así, para indicar que el marco 610 es un marco de información de tipo de autentificación de capa 2, el campo 612 de ID de CAP del ejemplo ilustrado almacena el identificador de capacidades (por ejemplo, ID de CAP = 270) que corresponde a la información 406 de tipo de autentificación de capa 2 de la estructura 400 de datos de capacidades de BSS de la figura 4.

El campo 614 de longitud almacena la longitud de bytes del marco 610 de información de tipo de autentificación de capa 2 para habilitar la recuperación de la misma de la memoria después de que el marco 610 es recibido por el terminal 114 inalámbrico. El campo 616 de conteo almacena la cantidad de IDs de AI a seguir en el marco 610 de información de tipo de autentificación de capa 2.

En el ejemplo ilustrado, cada uno de los campos de ID de AI (ID de AI #1 hasta ID de AI #M) en el marco 610 de información de tipo de autentificación de capa 2 almacena un único de los IDs 504 de AI de la estructura 500 de datos de AI de capa 2 para denotar uno o más de los tipos 502 de AI que son soportados y/o requeridos por el AP 104a. Un primero de los campos de ID de AI (es decir, ID de AI #1) se denota mediante el número de referencia 618 y su campo de valor de AI correspondiente (es decir, valor de AI #1) se denota mediante el número de referencia 620. Un segundo de los campos de ID de AI (es decir, ID de AI #2) se denota mediante el número de referencia 622 y su campo de valor de AI correspondiente (es decir, valor de AI #2) se denota mediante el número de referencia 624. En algunas implementaciones de ejemplo, el campo 618 de ID de AI #1 puede almacenar un identificador de ID de AI igual a 1, que corresponde al tipo 506 de AI de método de EAP como se muestra en la estructura 500 de datos de AI de capa 2 de la figura 5. En tales ejemplos, el campo 620 de valor de AI #1 puede almacenar el valor de formato entero de un protocolo de autentificación de EAP particular (por ejemplo, EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA, PEAP, etc.).

En el ejemplo ilustrado, el campo 622 de ID de AI #2 almacena un identificador de ID de AI igual a 5, que corresponde al tipo 514 de AI de AuP como se muestra en la estructura 500 de datos de AI de capa 2. Además, el campo 624 de valor de AI #2 almacena una lista 626 de AuP, que incluye uno o más AuPs separados por comas de la estructura 300 de datos de AuPs de la figura 3 (por ejemplo, NAI [ID de AuP = 1], SAN de servidor [ID de AuP = 3], etc.).

Con referencia ahora al intercambio de consulta/respuesta 606/608, para permitir que el terminal 114 inalámbrico descubra información de tipo de capa 3+, el AP 104a responde a la consulta 606 de capacidades comunicando un marco 628 de información de tipo de autentificación de capa 3+ al terminal 114 inalámbrico a través de la respuesta 608 de capacidades. En el ejemplo ilustrado, el marco 628 de información de tipo de autentificación de capa 3+ incluye un campo 630 de ID de CAP, un campo 632 de longitud, y una pluralidad de campos 634a y 634b de unidad de tipo de autentificación de capa 3+.

El campo 630 de ID de CAP identifica la capacidad de BSS con la cual está asociado el marco 628. Así, para indicar que el marco 628 es un marco de información de tipo de autentificación de capa 3+, el campo 630 de ID de CAP del ejemplo ilustrado almacena el identificador de capacidades (por ejemplo, ID de CAP = 260) que corresponde a la

entrada 404 de capacidad de información de tipo de autentificación de capa 3+ de la estructura 400 de datos de capacidades de BSS de la figura 4. El campo 632 de longitud almacena la longitud de bytes del marco 628 de información de tipo de autentificación de capa 3+ para habilitar la recuperación de la misma de la memoria después de que el marco 628 es recibido por el terminal 114 inalámbrico.

Cada uno de los campos 634a-b de unidad de tipo de autentificación de capa 3+ almacena un marco 636 de URL de redireccionamiento, del cual sólo se muestra uno. El marco 636 de URL de redireccionamiento puede ser usado para implementar otros procedimientos de autentificación cuando se requieren etapas adicionales para el acceso (por ejemplo, aceptar términos y condiciones, inscripción de inicio de sesión en línea, etc.) para establecer una conexión con el AP 104a. En el ejemplo ilustrado, el marco 636 de URL de redireccionamiento habilita la autentificación o procedimientos adicionales asociados con los procesos implementados en la capa 210 de aplicación de la arquitectura 200 de capa de comunicación de la figura 2. Tales procedimientos pueden ser adicionales o en vez de procesos de autentificación asociados con el marco 610 de información de tipo de autentificación de capa 2 discutido anteriormente. En algunas implementaciones de ejemplo, el marco 636 de URL de redireccionamiento puede especificar que un navegador web del terminal 114 inalámbrico debe desplegar términos y condiciones que deben ser aceptados por un usuario o una página de inscripción de inicio de sesión en línea en la cual un usuario debe iniciar sesión. El marco 636 de URL de redireccionamiento puede especificar adicional o alternativamente una redirección de HTTP/HTTPS y/o una redirección de servidor de nombres de dominio (DNS).

Pasando a las figuras 7-9, la figura 7 representa otra estructura 700 de datos de capacidades de conjunto de servicios básicos (BSS) de ejemplo, la figura 8 representa una estructura 800 de datos de información de autentificación (AI) de capa 2+ de ejemplo, y la figura 9 representa otro proceso de mensajería de ejemplo (por ejemplo, el cual puede ser usado para implementar la mensajería 206 de AI de la figura 2) para descubrir AI en un entorno de WLAN (por ejemplo, una de las ubicaciones 102a-c de acceso a WLAN de la figura 1). Como se discute a continuación, la estructura 700 de datos de capacidades de BSS es una versión modificada de la estructura 400 de datos de capacidades de BSS de la figura 4, y la estructura 800 de datos de AI de capa 2+ es una versión modificada de la estructura 500 de datos de AI de capa 2 de la figura 5.

A diferencia de la estructura 400 de datos de capacidades de BSS de la figura 4 que almacena la entrada 404 de capacidad de información de tipo de autentificación de capa 3+ separada de la entrada 406 de capacidad de información de tipo de autentificación de capa 2, la estructura 700 de datos de capacidades de BSS de la figura 7 almacena una entrada 702 de capacidad de información de tipo de autentificación de capa 2+. En el ejemplo ilustrado, la entrada 702 de capacidad de información de tipo de autentificación de capa 2+ indica que un AP (por ejemplo, los APs 104a-c de la figura 1) soporta todos los procesos y datos de autentificación (que involucran operaciones en o por encima de la subcapa 204 de MAC de la figura 2) que son indicados de otro modo por separado por la entrada 404 de capacidad de información de tipo de autentificación de capa 3+ y la entrada 406 de capacidad de información de tipo de autentificación de capa 2 de la figura 4. Es decir, la entrada 702 de capacidad de información de tipo de autentificación de capa 2+ indica que todos los tipos de AI de la estructura 500 de datos de AI de capa 2 de la figura 5 son combinados con la capacidad de redireccionamiento de URL descrita anteriormente en relación con el marco 636 de URL de redireccionamiento de la figura 6. De esta manera, cuando un terminal inalámbrico consulta a un AP las capacidades soportadas y/o requeridas asociadas con la autentificación, el terminal inalámbrico puede realizar una única consulta de GAS para descubrir toda la información de autentificación y/o parámetros discutidos anteriormente en relación con las figuras 3-6 en vez de dos consultas separadas como se describe en relación con la figura 6.

Para habilitar un descubrimiento de autentificación de consulta única, la estructura 800 de datos de AI de capa 2+ de la figura 8 es una versión modificada de la estructura 500 de datos de AI de capa 2 de la figura 5. Es decir, además de los tipos 506, 508, 510, 512, 514, y 516 de AI que se muestran en relación con la estructura 500 de datos de AI de capa 2, la estructura 800 de datos de AI de capa 2+ también incluye un tipo 802 de AI de URL de redireccionamiento, que corresponde a las capacidades de autentificación que de otro modo se indican mediante la entrada 404 de capacidad de información de tipo de autentificación de capa 3+ de la figura 4 y el marco 636 de URL de redireccionamiento de la figura 6.

Pasando ahora a la figura 9, el ejemplo ilustrado muestra un proceso 900 de intercambio de mensajería de consulta única que puede ser usado para descubrir requisitos de AI en una red inalámbrica en relación con las estructuras de datos descritas anteriormente en relación con las figuras 3, 7, y 8. Como se muestra, el proceso 900 de intercambio de mensajería de consulta única involucra una consulta 902 de capacidades única comunicada por el terminal 114 inalámbrico seguida por una respuesta 904 de capacidades única comunicada por el AP 104a. En el ejemplo ilustrado, las capacidades del AP 104a incluyen soporte para la información de tipo de autentificación de capa 2+ descrita anteriormente en relación con la entrada 702 de capacidad de información de tipo de autentificación de capa 2+ de la figura 7.

Como se muestra en la figura 9, un marco 906 de información de tipo de autentificación de capa 2+ comunicada a través de la respuesta 904 de capacidades es capaz de portar la misma información como se describió anteriormente en relación con el marco 610 de información de tipo de autentificación de capa 2 de la figura 6. Además, el marco 906 de información de tipo de autentificación de capa 2+ también es capaz de portar el marco 636 de URL de redireccionamiento descrito anteriormente en relación con el marco 628 de información de tipo de autentificación de

capa 3+ de la figura 6. En el ejemplo ilustrado, un campo 908 de ID de AI #3 almacena un valor de ID de AI de 6, que se muestra como que corresponde al tipo 802 de AI de URL de redireccionamiento en la figura 8.

Con referencia ahora a la figura 10, un ejemplo ilustrado del terminal 114 inalámbrico de las figuras 1, 6 y 9 se muestran en forma de diagrama de bloques. En el ejemplo ilustrado, el terminal 114 inalámbrico incluye un procesador 1002 que puede ser usado para controlar la operación general del terminal 114 inalámbrico. El procesador 1002 puede ser implementado usando un controlador, un procesador de propósito general, un procesador de señales digitales, o cualquier combinación de los mismos.

El terminal 114 inalámbrico también incluye un generador 1004 de mensajes de terminal y un analizador sintáctico 1006 de datos de terminal. El generador 1004 de mensajes de terminal puede ser usado para generar consultas (por ejemplo, las consultas 602 y 606 de la figura 6 y la consulta 902 de la figura 9) de acuerdo con cualquier protocolo de consulta incluyendo el formato de protocolo de consulta de GAS discutido anteriormente. El analizador sintáctico 1006 de datos de terminal puede ser usado para recuperar marcos de información de la memoria (por ejemplo, una RAM 1010) y recuperar información particular de interés de esos marcos. Por ejemplo, el analizador sintáctico 1006 de datos de terminal puede ser usado para recuperar AI y/o AuPs de cualquiera de los formatos de marco de datos discutidos anteriormente en relación con las figuras 6 y 9. Aunque el generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal se muestran como separados de y conectados al procesador 1002, en algunas implementaciones de ejemplo, el generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal pueden ser implementados en el procesador 1002 y/o en un subsistema de comunicación inalámbrica (por ejemplo, un subsistema 1018 de comunicación inalámbrica). El generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal pueden ser implementados usando cualquier combinación deseada de hardware, firmware, y/o software. Por ejemplo, pueden ser usados uno o más circuitos integrados, componentes semiconductores discretos, y/o componentes electrónicos pasivos. Así, por ejemplo, el generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal, o partes de los mismos, podrían ser implementados usando uno o más circuitos, procesadores programables, circuitos integrados de aplicación específica (ASICs), dispositivo lógicos programables (PLDs), dispositivo lógicos programables en campo (FPLDs), etc. El generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal, o partes de los mismos, pueden ser implementados usando instrucciones, código, y/u otro software y/o firmware, etc. almacenado en un medio accesible a máquina y ejecutable, por ejemplo, por un procesador (por ejemplo, el procesador 1002 de ejemplo). Cuando se lee cualquiera de las reivindicaciones anexas para cubrir una implementación puramente de software, al menos uno del generador 1004 de mensajes de terminal y el analizador sintáctico 1006 de datos de terminal se define expresamente por la presente para incluir un medio tangible tal como una memoria de estado sólido, una memoria magnética, un DVD, un CD, etc.

El terminal 114 inalámbrico también incluye una memoria FLASH 1008, una memoria de acceso aleatorio (RAM) 1010, y una interfaz de memoria expandible 1012 acoplada de manera comunicativa al procesador 1002. La memoria FLASH 1008 puede ser usada para, por ejemplo, almacenar instrucciones legibles por ordenador y/o datos. En algunas implementaciones de ejemplo, la memoria FLASH 1008 puede ser usada para almacenar una o más de las estructuras de datos discutidas anteriormente en relación con las figuras 3, 4, 5, 7, y 8 y también puede almacenar valores de AuP asociados con el terminal 114 inalámbrico. La RAM 1010 también puede ser usad para, por ejemplo, almacenar datos y/o instrucciones.

El terminal 114 inalámbrico está provisto de una interfaz 1014 de hardware de seguridad para recibir una tarjeta de SIM (o una tarjeta de USIM o un elemento seguro de NFC) de un proveedor de servicios inalámbricos. Como se discutió anteriormente, una tarjeta de SIM puede ser usada como un parámetro de autentificación para autentificar el terminal 114 inalámbrico para establecer una conexión con una red soportada con WLAN. El terminal 114 inalámbrico también está provisto de una interfaz 1016 de E/S de datos externos. La interfaz 1016 de E/S de datos externos puede ser usada por un usuario para transferir información al terminal 114 inalámbrico a través de un medio por cable. Una trayectoria de transferencia de datos por cable puede ser usada, por ejemplo, para cargar una clave de encriptado u otro tipo de AuP en el terminal 114 inalámbrico a través de una conexión directa y, así, fiable y de confianza para proporcionar comunicación segura de dispositivo.

El terminal 114 inalámbrico está provisto de un subsistema 1018 de comunicación inalámbrica para habilitar las comunicaciones inalámbricas con APs de WLAN (por ejemplo, los APs 104a-c de la figura 1). Aunque no se muestra, el terminal 114 inalámbrico también puede tener un subsistema de comunicación de largo alcance para recibir mensajes desde, y enviar mensajes a, una red inalámbrica celular. En los ejemplos ilustrados descritos en este documento, el subsistema 1018 de comunicación inalámbrica puede estar configurado de acuerdo con el estándar IEEE® 802.11. En otras implementaciones de ejemplo, el subsistema 1018 de comunicación inalámbrica puede ser implementado usando una radio BLUETOOTH®, un dispositivo ZIGBEE®, un dispositivo de USB inalámbrico, o una radio de ultra banda ancha (UWB).

Para habilitar que un usuario use e interactúe con o a través del terminal 114 inalámbrico, el terminal 114 inalámbrico está provisto de un altavoz 1020, un micrófono 1022, una pantalla 1024, y una interfaz 1026 de entrada de usuario. La pantalla 1024 puede ser una pantalla LCD, una pantalla de e-paper, etc. La interfaz 1026 de entrada de usuario podría ser un teclado alfanumérico y/o un teclado numérico tipo teléfono, un accionador multidirección o una rueda giratoria con capacidad para presionar botones dinámicos, un panel táctil, etc. En el ejemplo ilustrado, el terminal 114

inalámbrico es un dispositivo alimentado por batería y está, así, provisto de una batería 1028 y una interfaz 1030 de batería.

Pasando ahora a la figura 11, el AP 104a de ejemplo de las figuras 1, 6, y 9 se muestra en forma de diagrama de bloques. El AP 104a de ejemplo incluye un procesador 1102 para realizar las operaciones generales del AP 104a. Además, el AP 104a incluye un generador 1104 de mensajes de AP para generar mensajes de consulta y/o respuesta y un analizador sintáctico 1106 de datos de AP para recuperar información de marcos de datos recibidos. El generador 1104 de mensajes de AP es sustancialmente similar al generador 1004 de mensajes de terminal de la figura 10, y el analizador sintáctico 1106 de datos de AP es sustancialmente similar al analizador sintáctico 1006 de datos de terminal de la figura 10. Así, el generador 1104 de mensajes de AP y el analizador sintáctico 1106 de datos de AP pueden ser implementados en el procesador 1102 y/o un subsistema de comunicación inalámbrica (por ejemplo, un subsistema 1112 de comunicación inalámbrica) usando cualquier combinación de hardware, firmware, y/o software incluyendo las instrucciones almacenadas en un medio legible por ordenador.

El AP 104a de ejemplo también incluye una memoria FLASH 1108 y una RAM 1110, ambas de las cuales están acopladas al procesador 1102. La memoria FLASH 1108 puede estar configurada para almacenar AuPs requeridos de la estructura de datos de AuP de la figura 300, indicadores de capacidad soportados de las estructuras 400 o 700 de datos de capacidades de BSS, y tipos de AI soportados de las estructuras 500 u 800 de datos.

Para comunicarse con terminales inalámbricos tales como el terminal 114 inalámbrico, el AP 104a está provisto de un subsistema 1112 de comunicación inalámbrica, el cual puede ser sustancialmente similar o idéntico al subsistema 1018 de comunicación inalámbrica (figura 10) del terminal 114 inalámbrico. Para comunicarse con una red soportada con WLAN (por ejemplo, las redes 106a-b, 110, y 108a-b), el AP 104a está provisto de una interfaz 1114 de comunicación de enlace ascendente de red.

La figura 12 representa un diagrama de flujo de ejemplo representativo de instrucciones legibles por ordenador que pueden ser usadas para descubrir AuPs asociados con el acceso a una red soportada con WLAN (por ejemplo, las redes 106a-b, 108a-b, y 110 de la figura 1). Las operaciones de ejemplo de la figura 12 puede ser realizadas usando un procesador, un controlador y/o cualquier otro dispositivo de procesamiento adecuado. Por ejemplo, las operaciones de ejemplo de la figura 12 pueden ser implementadas usando instrucciones codificadas almacenadas en un medio tangible tal como una memoria flash, una memoria de solo lectura (ROM) y/o memoria de acceso aleatorio (RAM) asociada con un procesador (por ejemplo, el procesador 1002 de la figura 10 y/o el procesador 1102 de la figura 11). Alternativamente, algunas o todas las operaciones de ejemplo de la figura 12 pueden ser implementadas usando cualquier combinación de circuitos integrados de aplicación específica (ASICs), dispositivos lógicos programables (PLDs), dispositivos lógicos programables en campo (FPLDs), lógica discreta, hardware, firmware, etc. También, algunas o todas las operaciones de ejemplo de la figura 12 puede ser implementadas manualmente o como cualquier combinación de cualquiera de las técnicas anteriores, por ejemplo, cualquier combinación de firmware, software, lógica discreta y/o hardware. Adicionalmente, aunque las operaciones de ejemplo de la figura 12 se describen con referencia al diagrama de flujo de la figura 12, otros métodos de implementación de las operaciones de la figura 12 pueden ser empleados. Por ejemplo, el orden de ejecución de los bloques puede ser cambiado, y/o algunos de los bloques descritos pueden ser cambiados, eliminados, subdivididos, o combinados. Adicionalmente, cualquiera o todas las operaciones de ejemplo de la figura 12 pueden ser realizadas de manera secuencial y/o en paralelo por, por ejemplo, hilos de procesamiento separados, procesadores, dispositivos, lógica discreta, circuitos, etc.

En general, el diagrama de flujo de ejemplo de la figura 12 puede ser usado para implementar el proceso 600 de intercambio de mensajería de ejemplo de la figura 6 y/o el proceso 900 de intercambio de mensajería de ejemplo de la figura 9 durante un proceso de descubrimiento de WLAN. El diagrama de flujo de ejemplo de la figura 12 incluye un proceso 1202 de terminal inalámbrico y un proceso 1204 de AP. El proceso 1202 de terminal inalámbrico puede ser implementado usando el terminal 114 inalámbrico (figuras 1, 6, 9, y 10) para consultar el AP 104a para descubrir AuPs requeridos por el AP 104a. El proceso 1204 de AP puede ser implementado usando el AP 104a (figuras 1, 6, 9, y 11) para transmitir la AI y/o AuPs requeridos por el AP 104a.

Pasando en detalle a la figura 12, inicialmente, el terminal 114 inalámbrico transmite una solicitud de sonda (bloque 1206) a través del subsistema 1018 de comunicación inalámbrica. En el ejemplo ilustrado, la solicitud de sonda es usada para consultar al AP 104a si soporta el interfuncionamiento con redes externas (por ejemplo, las redes 106a-b, 108a-b, y 110). El AP 104a recibe la solicitud de sonda (bloque 1208) a través del subsistema 1112 de comunicación inalámbrica y transmite una respuesta de sonda (bloque 1210) para indicar si soporta el interfuncionamiento con redes externas y si requiere autentificación.

El terminal 114 inalámbrico recibe la respuesta de sonda (bloque 1212) a través del subsistema 1018 de comunicación inalámbrica y el analizador sintáctico 1006 de datos de terminal (figura 1) analiza de manera sintáctica la respuesta de sonda para determinar si se requiere autentificación (bloque 1214). Por ejemplo, la respuesta de sonda puede incluir un campo de bits de Etapa Adicional Requerida para Acceso (ASRA) (por ejemplo, un campo de bits de requerido para autentificación) (no se muestra) para indicar si se requiere autentificación. Cuando se requiere autentificación (bloque 1212) (por ejemplo, el campo de bits de ASRA es verdadero), el terminal 114 inalámbrico transmite un mensaje de solicitud de capacidades de autentificación (bloque 1216) (por ejemplo, una de las consultas

602 de la figura 6 o 902 de la figura 9) usando, por ejemplo, una consulta de GAS. El terminal 114 inalámbrico luego espera hasta que recibe una respuesta (bloque 1218).

El AP 104a recibe el mensaje de solicitud de capacidades de autentificación (bloque 1220), y el generador 1104 de mensajes de AP (figura 11) empaqueta o inserta los identificadores de AI y AuP requeridos en un mensaje de respuesta de capacidades de autentificación (bloque 1222) (por ejemplo, una de las respuestas 604 de capacidades de la figura 6 o 904 de la figura 9). Los identificadores de AI y AuP asociados con el AP 104a pueden ser almacenados en una memoria (por ejemplo, una de la memoria flash 1108 o la RAM 1110 de la figura 11) del AP 104a. El AP 104a luego transmite el mensaje de respuesta de capacidades de autentificación (bloque 1224).

Si el método de ejemplo de la figura 12 es implementado usando la técnica de descubrimiento de AI descrita anteriormente en relación con las figuras 4-6, el mensaje de solicitud de capacidades de autentificación del bloque 1216 es la consulta 602 de capacidades de la figura 6, el mensaje de respuesta de capacidades de autentificación de bloque 1222 es la respuesta 604 de capacidades de la figura 6, y el mensaje de respuesta de capacidades de autentificación es implementado usando el formato del marco 610 de información de tipo de autentificación de capa 2 de la figura 6. Si el método de ejemplo de la figura 12 es implementado usando la técnica de descubrimiento de AI descrita anteriormente en relación con las figuras 7-9, el mensaje de solicitud de capacidades de autentificación de bloque 1216 es la consulta 902 de capacidades de la figura 9, el mensaje de respuesta de capacidades de autentificación de bloque 1224 es la respuesta 904 de capacidades de la figura 9, y el mensaje de respuesta de capacidades de autentificación es implementado usando el formato del marco 906 de información de tipo de autentificación de capa 2+ de la figura 9.

Cuando el terminal 114 inalámbrico recibe el mensaje de respuesta de capacidades de autentificación (bloque 1218), el analizador sintáctico 1006 de datos de terminal (figura 10) recupera los identificadores de AI y AuP del marco de mensaje recibido (bloque 1226). Si el terminal 114 inalámbrico determina que tiene los valores de AI y/o AuP requeridos indicados por los identificadores de AI y AuP recibidos (bloque 1228), el generador 1004 de mensajes de terminal (figura 10) empaqueta o inserta los valores de AI y/o AuP en un mensaje de solicitud de conexión (bloque 1230). Por ejemplo, el terminal 114 inalámbrico puede ejecutar uno o más procesos de recuperación de valores de autentificación que realizan operaciones en la subcapa 204 de MAC para recuperar los valores de AI y/o AuP sin necesidad de permitir que los procesos de recuperación de valores de autentificación realicen operaciones en o por encima de una capa de protocolo de internet (IP) (por ejemplo, la capa 208 de red de la figura 2) sin necesidad de proporcionar de otra manera los procesos de recuperación de valor de autentificación con acceso a la capa de IP.

En algunas implementaciones de ejemplo, cuando el terminal 114 inalámbrico determina en el bloque 1228 que tiene los valores de AI y/o AuP requeridos, un usuario puede ser avisado con el SSID (o HESSID) asociado con el AP 104a antes de generar el mensaje de solicitud de conexión. De esta manera, se le puede dar al usuario la opción de si conectarse al AP 104a en vez de permitir que el terminal 114 inalámbrico se conecte automáticamente al AP 104a. En algunas implementaciones de ejemplo, si el terminal 114 inalámbrico determina en el bloque 1228 que no tiene los valores de AI y/o AuP requeridos, el terminal 114 inalámbrico (por ejemplo, el procesador 1002 de la figura 10) puede abstenerse de desplegar el SSID (o HESSID) asociado con el AP 104a. De esta manera, la red 106a privada no se muestra como disponible para conectarse dado que el terminal 114 inalámbrico no podría conectarse a esta sin los valores de AI y/o AuP requeridos. Además, en algunas implementaciones de ejemplo, el terminal 114 inalámbrico puede estar configurado para almacenar los identificadores de AI y AuP obtenidos en el bloque 1226 en relación con un SSID del AP 104a como un perfil para el AP 104a. De esta manera, cuando el terminal 114 inalámbrico redescubre subsecuentemente la presencia del AP 104a, el terminal 114 inalámbrico puede usar los identificadores de AI y AuP almacenados para determinar los valores de AI y/o AuP que debe proporcionar al AP 104a para ser autentificado sin tener que resolicitar AI y/o AuPs requeridos del AP 104a.

Después de que los valores de AI y/o AuP son empaquetados o insertados en un mensaje de solicitud de conexión (bloque 1230) o si el terminal 114 inalámbrico determinó en el bloque 1214 que el AP 104a no requiere autentificación, el terminal 114 inalámbrico transmite el mensaje de solicitud de conexión (bloque 1232). Después de que el AP 104a recibe el mensaje de solicitud de conexión (bloque 1234), el analizador sintáctico 1106 de datos de AP (figura 11) analiza de manera sintáctica los valores de AI y/o AuP del mensaje de solicitud de conexión (bloque 1236) y el AP 104a (u otro sistema u ordenador interconectado al AP 104a) realiza un proceso de autentificación (bloque 1238). Luego el AP 104a autentifica y establece una conexión con el terminal 114 inalámbrico o niega una conexión con el terminal 114 inalámbrico con base en si los valores de AI y/o AuP proporcionados por el terminal 114 inalámbrico fueron satisfactorios para autentificación.

Después de que el AP 104a se conecta al terminal 114 inalámbrico o niega la conexión (bloque 1240), o si el terminal 114 inalámbrico determina que no tiene los valores de AI y/o AuP requeridos, finaliza el proceso de ejemplo de la figura 12.

REIVINDICACIONES

1. Un método para proporcionar información de autentificación de red en una red inalámbrica, comprendiendo el método:

recibir, por un punto de acceso, durante el descubrimiento de red y antes de la autentificación, una solicitud de Servicio de Anuncio Genérico, GAS, desde un terminal inalámbrico, solicitando la solicitud de GAS información de autentificación de red; y

transmitir, por el punto de acceso y al terminal inalámbrico, una respuesta a la solicitud de GAS, en donde la respuesta incluye la información de autentificación de red, en donde la información de autentificación de red incluye información de tipo de autentificación y un marco de localizador de recursos uniforme de redireccionamiento, URL, en donde la información de tipo de autentificación indica que el terminal inalámbrico usa el marco de URL de redireccionamiento para obtener términos y condiciones.

2. El método de la reivindicación 1, en donde la información de tipo de autentificación indica además que el terminal inalámbrico realiza al menos una de: (a) inscripción de inicio de sesión en línea, o (b) redirección de servidor de nombres de dominio, DNS.

3. El método de la reivindicación 1, en donde la información de autentificación de red incluye un campo de longitud de URL de redireccionamiento.

4. El método de la reivindicación 1, en donde el terminal inalámbrico es un dispositivo de comunicación móvil.

5. Un punto de acceso que proporciona información de autentificación de red en una red inalámbrica, que comprende:

una memoria; y

al menos un procesador de hardware acoplado de manera comunicativa con la memoria y configurado para:

recibir, durante el descubrimiento de red y antes de la autentificación, una solicitud de Servicio de Anuncio Genérico, GAS, desde un terminal inalámbrico, solicitando la solicitud de GAS información de autentificación de red; y

transmitir, al terminal inalámbrico, una respuesta a la solicitud de GAS, en donde la respuesta incluye la información de autentificación de red, en donde la información de autentificación de red incluye información de tipo de autentificación y un marco de localizador de recursos uniforme de redireccionamiento, URL, en donde la información de tipo de autentificación indica que el terminal inalámbrico usa el marco de URL de redireccionamiento para obtener términos y condiciones.

6. El punto de acceso de la reivindicación 5, en donde la información de tipo de autentificación indica además que el terminal inalámbrico realiza al menos una de: (a) inscripción de inicio de sesión en línea, o (b) redirección de servidor de nombres de dominio, DNS.

7. El punto de acceso de la reivindicación 5, en donde la información de autentificación de red incluye un campo de longitud de URL de redireccionamiento.

8. El punto de acceso de la reivindicación 5, en donde el punto de acceso es un punto de acceso inalámbrico.

9. Un medio legible por ordenador que tiene instrucciones almacenadas en el mismo que, cuando se ejecutan, hacen que un procesador opere de acuerdo con el método de cualquiera de las reivindicaciones 1 a 4.

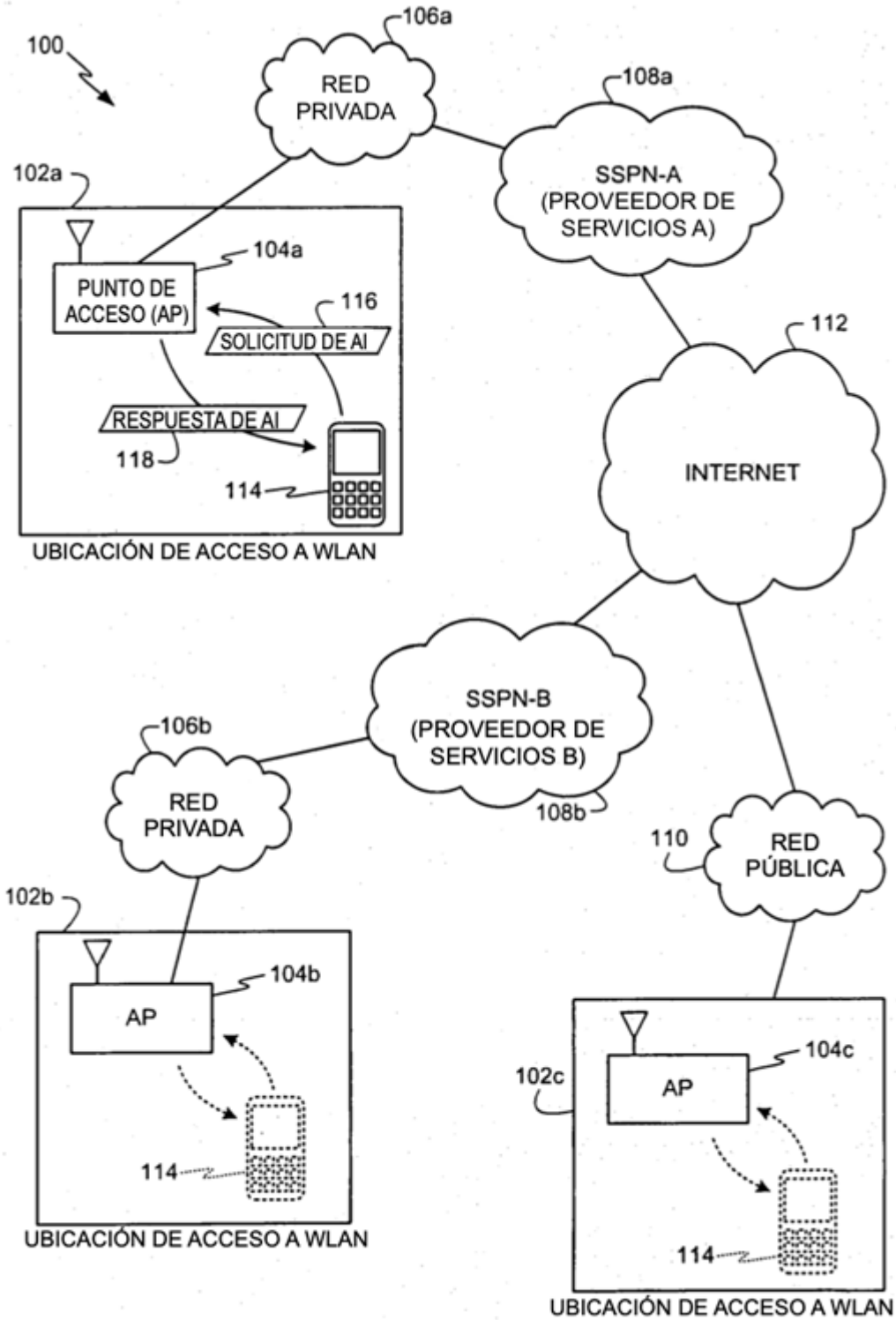
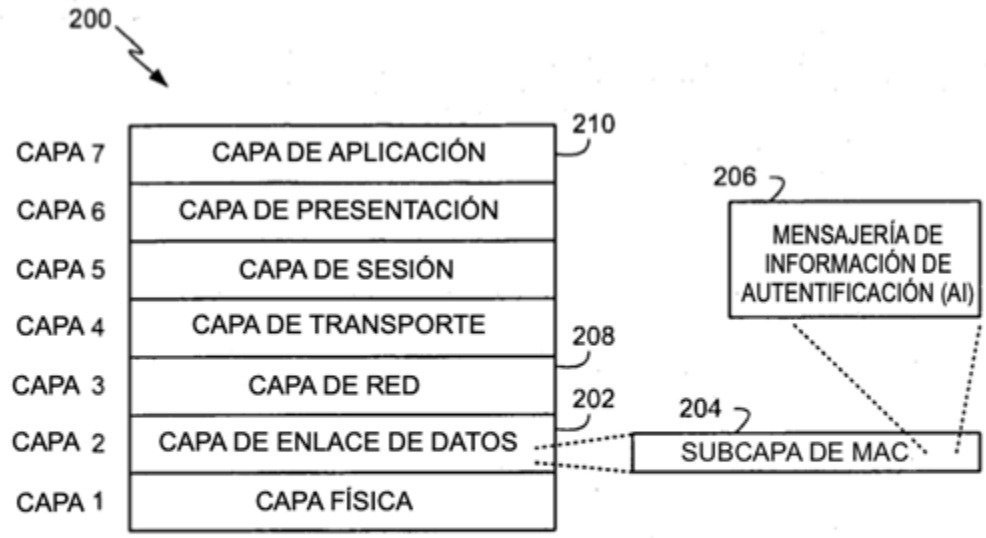

100
106a
RED PRIVADA
108a
SSPN-A (PROVEEDOR DE SERVICIOS A)
102a
PUNTO DE ACCESO (AP)
104a
116
SOLICITUD DE AI
RESPUESTA DE AI
118
114
UBICACIÓN DE ACCESO A WLAN
112
INTERNET
SSPN-B (PROVEEDOR DE SERVICIOS B)
108b
106b
RED PRIVADA
110
RED PÚBLICA
102b
AP
104b
114
UBICACIÓN DE ACCESO A WLAN
102c
AP
104c
114
UBICACIÓN DE ACCESO A WLAN

FIG. 1



ARQUITECTURA DE CAPA DE COMUNICACIÓN

FIG. 2

302 304

NOMBRE DE AuP	ID DE AuP
INDICADOR DE DIRECCIÓN DE RED (NAI)	1
ASUNTO DE SERVIDOR	2
RED DE ÁREA DE ALMACENAMIENTO DE SERVIDOR (SAN)	3
ESPECÍFICO DE VENDEDOR	255

PARÁMETROS DE AUTENTIFICACIÓN (AuPs)

300

FIG. 3

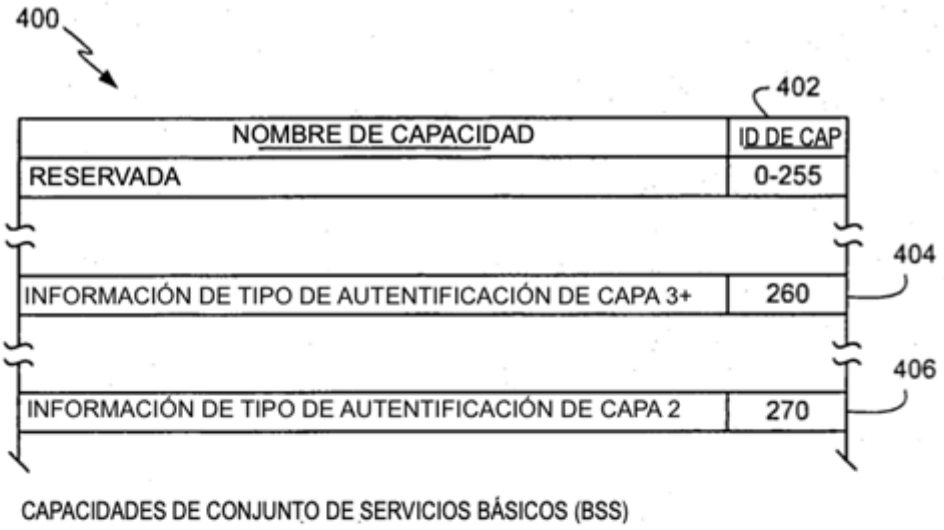
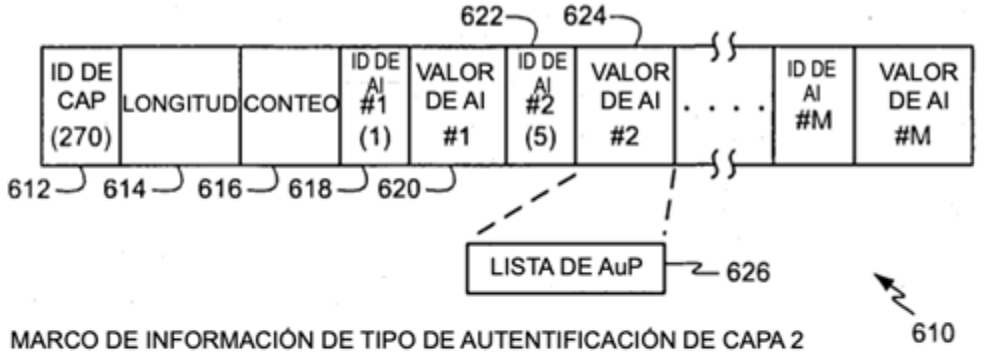

400
402
NOMBRE DE CAPACIDAD
ID DE CAP
RESERVADA
0-255
404
INFORMACIÓN DE TIPO DE AUTENTIFICACIÓN DE CAPA 3+
260
406
INFORMACIÓN DE TIPO DE AUTENTIFICACIÓN DE CAPA 2
270
CAPACIDADES DE CONJUNTO DE SERVICIOS BÁSICOS (BSS)

FIG. 4


502
504
TIPO DE AI
ID DE AI
FORMATO
506
NOMBRE DE MÉTODO DE EAP
1
ENTERO
508
MODO DE AUTENTIFICACIÓN INTERNA
2
CADENA
510
TIPO CERTIFICADO
3
CADENA
512
HARDWARE DE SEGURIDAD
4
TIPO DE ENUM.
(1-SIM, 2-USIM, 3-ELEMENTO SEGURO DE NFC, 4-CONTRASEÑA DE HARDWARE)
514
PARÁMETRO DE AUTENTIFICACIÓN (AuP)
5
CADENA (LISTA DE INDICADORES DE AuP SEPARADOS POR COMAS)
516
ESPECÍFICO DE VENDEDOR
255
CADENA
INFORMACIÓN DE AUTENTIFICACIÓN (AI) DE CAPA 2

500

FIG. 5


622
624
ID DE CAP (270)
LONGITUD
CONTEO
ID DE AI #1 (1)
VALOR DE AI #1
ID DE AI #2 (5)
VALOR DE AI #2
ID DE AI #M
VALOR DE AI #M
612
614
616
618
620
LISTA DE AuP
626
MARCO DE INFORMACIÓN DE TIPO DE AUTENTIFICACIÓN DE CAPA 2
610

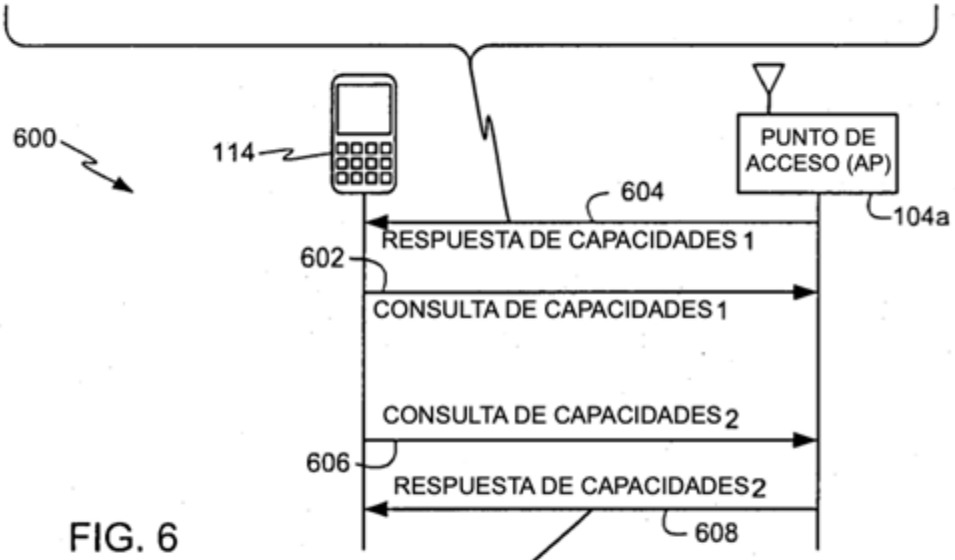
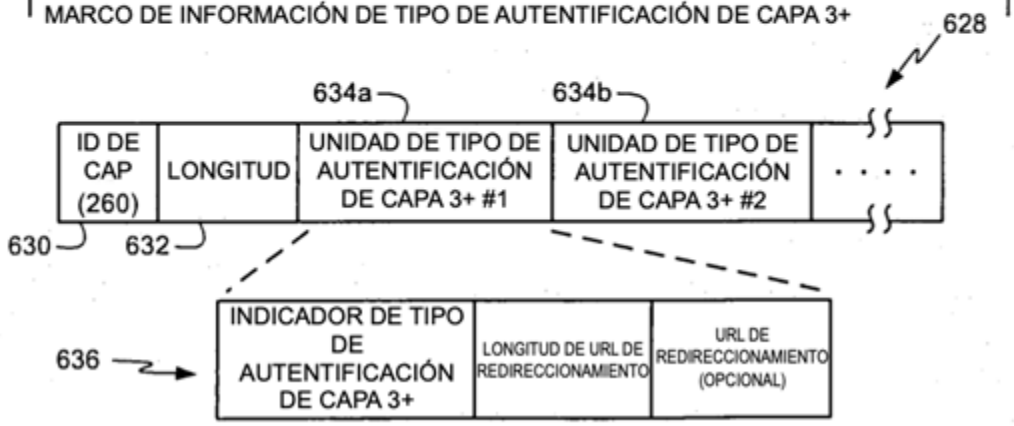

600
114
PUNTO DE ACCESO (AP)
104a
604
RESPUESTA DE CAPACIDADES 1
602
CONSULTA DE CAPACIDADES 1
CONSULTA DE CAPACIDADES 2
606
RESPUESTA DE CAPACIDADES 2
608

FIG. 6


MARCO DE INFORMACIÓN DE TIPO DE AUTENTIFICACIÓN DE CAPA 3+
628
634a
634b
ID DE CAP (260)
LONGITUD
UNIDAD DE TIPO DE AUTENTIFICACIÓN DE CAPA 3+ #1
UNIDAD DE TIPO DE AUTENTIFICACIÓN DE CAPA 3+ #2
630
632
636
INDICADOR DE TIPO DE AUTENTIFICACIÓN DE CAPA 3+
LONGITUD DE URL DE REDIRECCIONAMIENTO
URL DE REDIRECCIONAMIENTO (OPCIONAL)

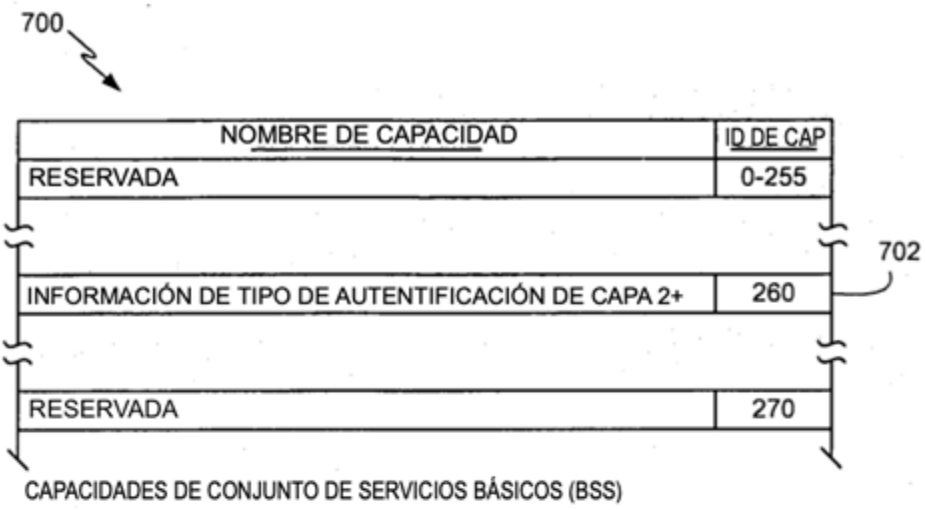


FIG. 7

800

TIPO DE AI	ID DE AI	FORMATO
NOMBRE DE MÉTODO DE EAP	1	ENTERO
MODO DE AUTENTIFICACIÓN INTERNA	2	CADENA
TIPO CERTIFICADO	3	CADENA
HARDWARE DE SEGURIDAD	4	TIPO DE ENUM. (1-SIM, 2-USIM, 3-ELEMENTO SEGURO DE NFC, 4-CONTRASEÑA DE HARDWARE)
PARÁMETRO DE AUTENTIFICACIÓN (AuP)	5	CADENA (LISTA DE INDICADORES DE AuP SEPARADOS POR COMAS)
URL DE REDIRECCIONAMIENTO	6	CADENA
ESPECÍFICO DE VENDEDOR	255	CADENA

802

INFORMACIÓN DE AUTENTIFICACIÓN (AI) DE CAPA 2+

FIG. 8

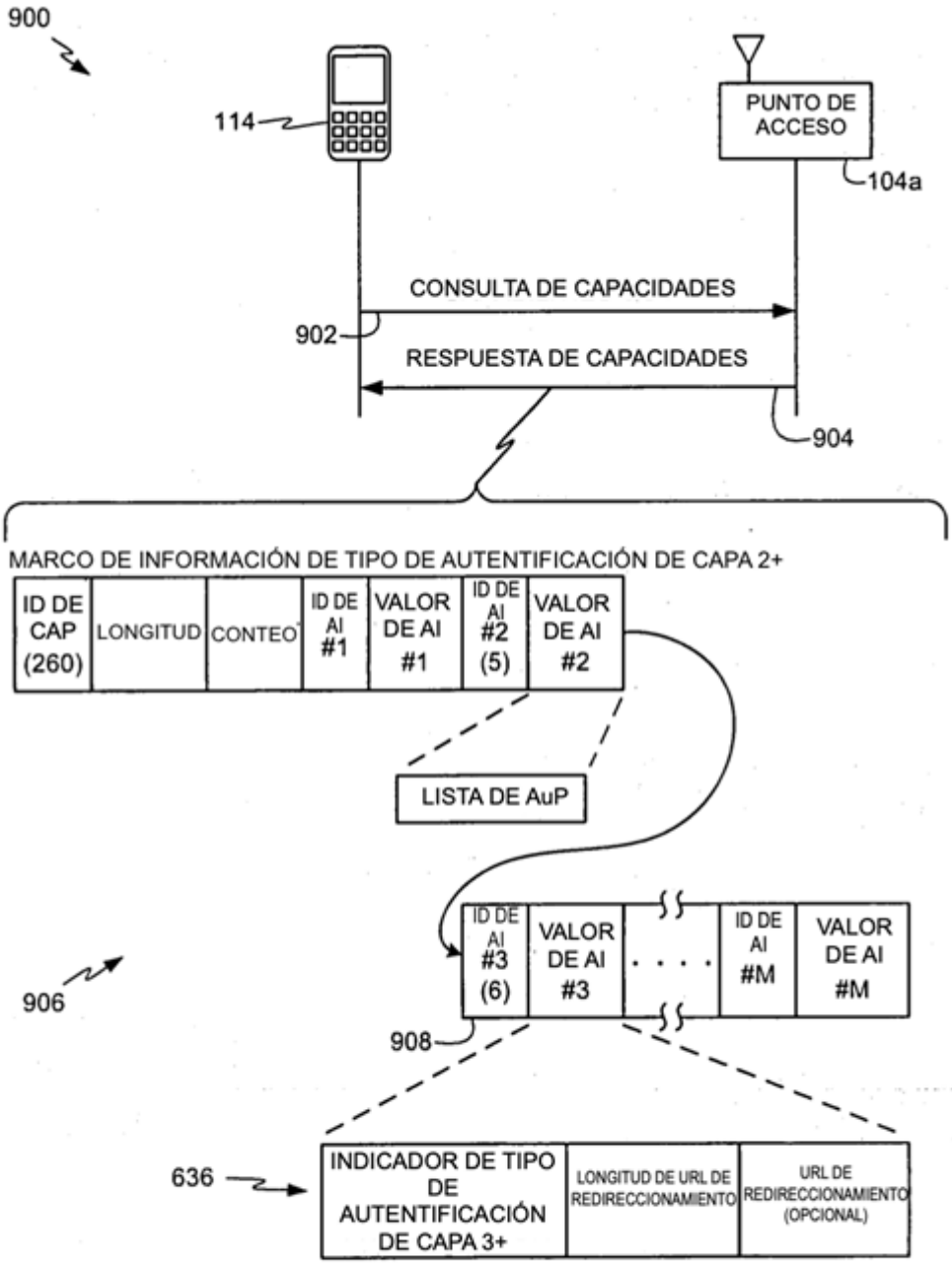

900
114
PUNTO DE ACCESO
104a
CONSULTA DE CAPACIDADES
902
RESPUESTA DE CAPACIDADES
904
MARCO DE INFORMACIÓN DE TIPO DE AUTENTIFICACIÓN DE CAPA 2+
ID DE CAP (260)
LONGITUD
CONTEO
ID DE AI #1
VALOR DE AI #1
ID DE AI #2 (5)
VALOR DE AI #2
LISTA DE AuP
906
ID DE AI #3 (6)
VALOR DE AI #3
ID DE AI #M
VALOR DE AI #M
908
636
INDICADOR DE TIPO DE AUTENTIFICACIÓN DE CAPA 3+
LONGITUD DE URL DE REDIRECCIONAMIENTO
URL DE REDIRECCIONAMIENTO (OPCIONAL)

FIG. 9

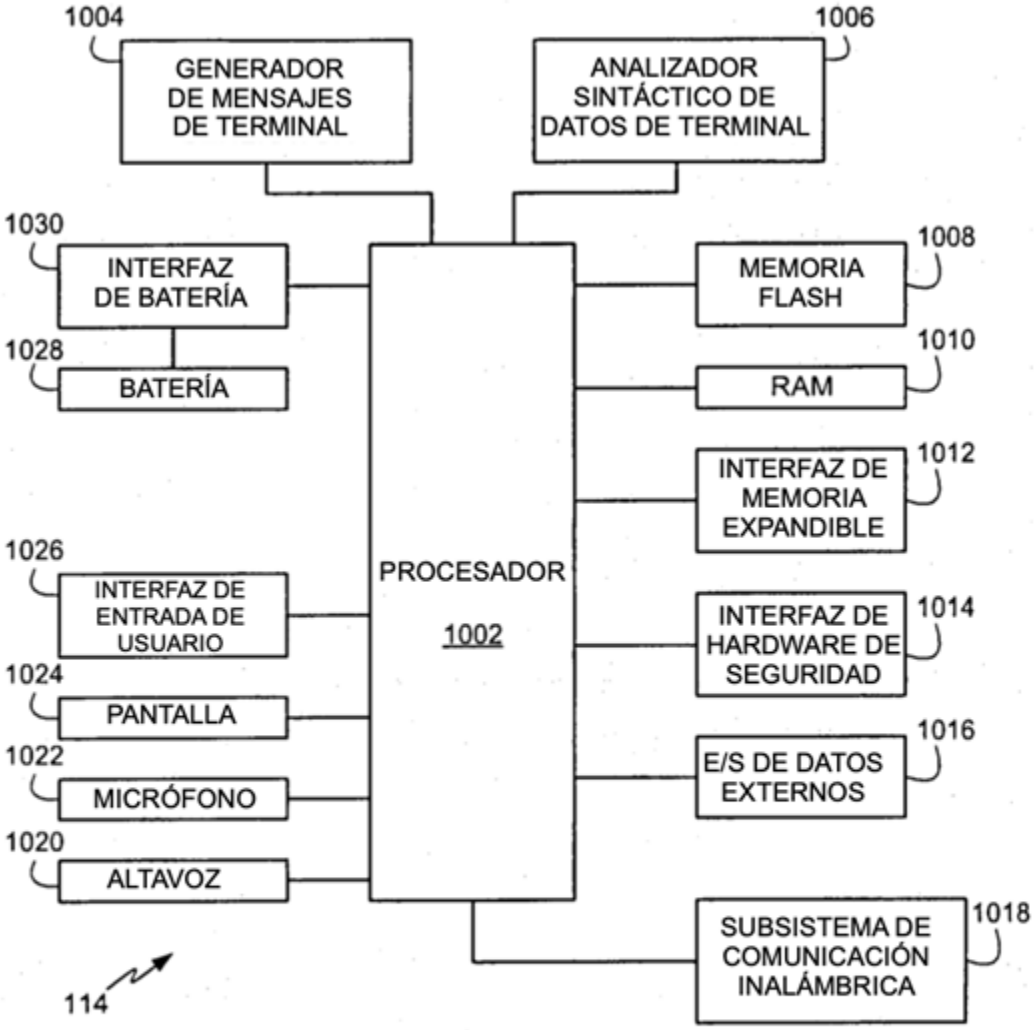

1004
GENERADOR DE MENSAJES DE TERMINAL
1006
ANALIZADOR SINTÁCTICO DE DATOS DE TERMINAL
1030
INTERFAZ DE BATERÍA
1028
BATERÍA
1026
INTERFAZ DE ENTRADA DE USUARIO
1024
PANTALLA
1022
MICRÓFONO
1020
ALTAVOZ
PROCESADOR
1002
1008
MEMORIA FLASH
1010
RAM
1012
INTERFAZ DE MEMORIA EXPANDIBLE
1014
INTERFAZ DE HARDWARE DE SEGURIDAD
1016
E/S DE DATOS EXTERNOS
1018
SUBSISTEMA DE COMUNICACIÓN INALÁMBRICA
114
TERMINAL INALÁMBRICO

FIG. 10

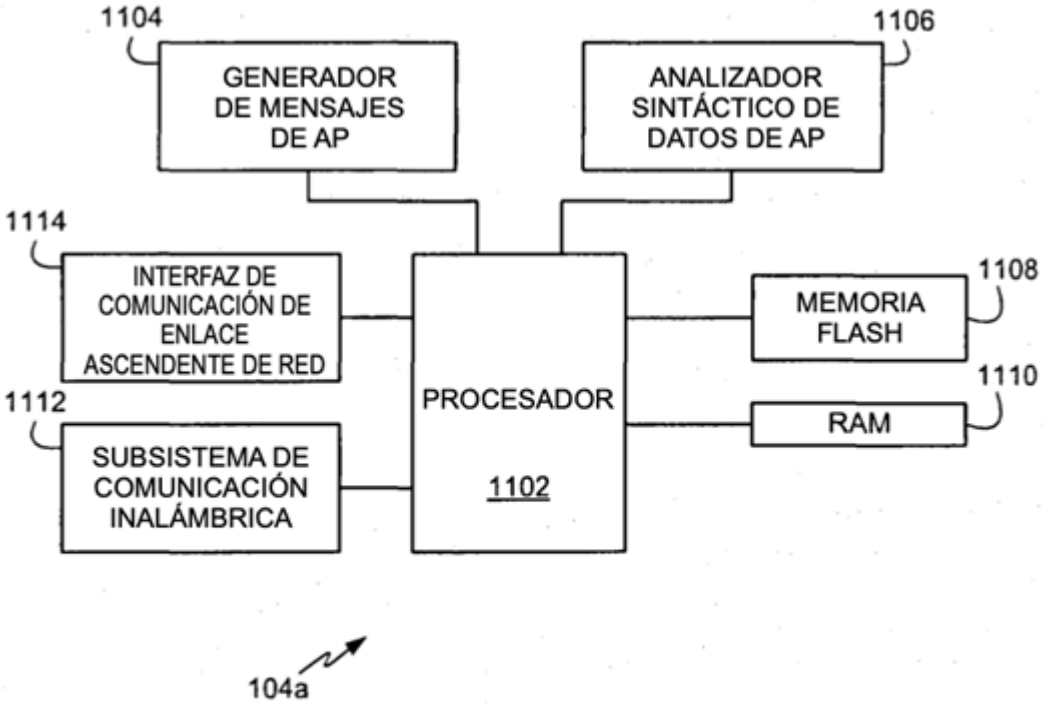

1104
GENERADOR DE MENSAJES DE AP
1106
ANALIZADOR SINTÁCTICO DE DATOS DE AP
1114
INTERFAZ DE COMUNICACIÓN DE ENLACE ASCENDENTE DE RED
1112
SUBSISTEMA DE COMUNICACIÓN INALÁMBRICA
PROCESADOR
1102
1108
MEMORIA FLASH
1110
RAM
104a
PUNTO DE ACCESO

FIG. 11

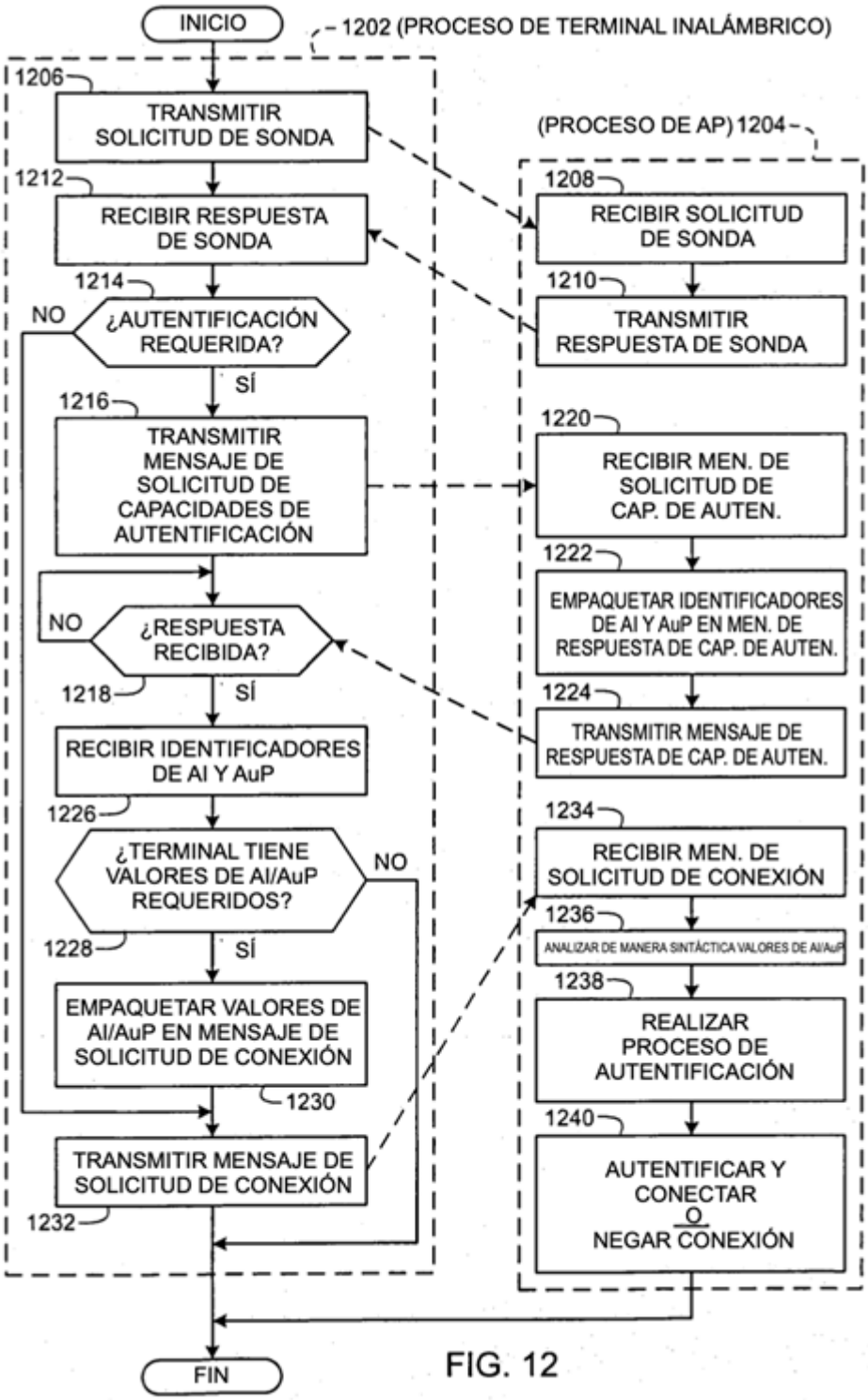

INICIO
1202 (PROCESO DE TERMINAL INALÁMBRICO)
1206
TRANSMITIR SOLICITUD DE SONDA
1212
RECIBIR RESPUESTA DE SONDA
1214
NO
¿AUTENTIFICACIÓN REQUERIDA?
SÍ
1216
TRANSMITIR MENSAJE DE SOLICITUD DE CAPACIDADES DE AUTENTIFICACIÓN
NO
¿RESPUESTA RECIBIDA?
1218
SÍ
RECIBIR IDENTIFICADORES DE AI Y AuP
1226
¿TERMINAL TIENE VALORES DE AI/AuP REQUERIDOS?
NO
1228
SÍ
EMPAQUETAR VALORES DE AI/AuP EN MENSAJE DE SOLICITUD DE CONEXIÓN
1230
TRANSMITIR MENSAJE DE SOLICITUD DE CONEXIÓN
1232
(PROCESO DE AP) 1204
1208
RECIBIR SOLICITUD DE SONDA
1210
TRANSMITIR RESPUESTA DE SONDA
1220
RECIBIR MEN. DE SOLICITUD DE CAP. DE AUTEN.
1222
EMPAQUETAR IDENTIFICADORES DE AI Y AuP EN MEN. DE RESPUESTA DE CAP. DE AUTEN.
1224
TRANSMITIR MENSAJE DE RESPUESTA DE CAP. DE AUTEN.
1234
RECIBIR MEN. DE SOLICITUD DE CONEXIÓN
1236
ANALIZAR DE MANERA SINTÁCTICA VALORES DE AI/AuP
1238
REALIZAR PROCESO DE AUTENTIFICACIÓN
1240
AUTENTIFICAR Y CONECTAR
O
NEGAR CONEXIÓN
FIN

FIG. 12