(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 643 290**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 12/04 (2009.01)
H04L 9/08 (2006.01)
H04W 36/14 (2009.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04W 84/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2012 E 14183535 (5)**

(97) Fecha y número de publicación de la concesión europea: **05.07.2017 EP 2827630**

(54) Título: **Sistemas y procedimientos de realización de la configuración y autentificación de enlaces**

(30) Prioridad:

12.09.2011 US 201161533627 P
15.09.2011 US 201161535234 P
04.01.2012 US 201261583052 P
05.03.2012 US 201261606794 P
15.03.2012 US 201261611553 P
11.05.2012 US 201261645987 P
11.09.2012 US 201213610730

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.11.2017

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121, US

(72) Inventor/es:

CHERIAN, GEORGE;
HAWKES, PHILIP MICHAEL;
ABRAHAM, SANTOSH PAUL y
SAMPATH, HEMANTH

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Sistemas y procedimientos de realización de la configuración y autentificación de enlaces

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

[0001] La presente solicitud reivindica prioridad de la Solicitud de Patente Provisional de Estados Unidos de propiedad común 61/533 627 (número de expediente Qualcomm 113346P1) presentada el 12 de septiembre del 2011, la Solicitud de Patente Provisional de Estados Unidos 61/535 234 (número de expediente Qualcomm 113346P2) presentada el 15 de septiembre de 2011, la Solicitud de Patente Provisional de Estados Unidos 61/583 052 (número de expediente Qualcomm 113346P3), presentada el 4 de enero de 2012, la Solicitud de Patente Provisional de Estados Unidos 61/606 794 (número de expediente Qualcomm 121585P1) presentada el 5 de marzo de 2012, la Solicitud de Patente Provisional de Estados Unidos 61/645 987 (número de expediente Qualcomm 121585P2) presentada el 11 de mayo de 2012, y la Solicitud de Patente Provisional de Estados Unidos 61/611 553 (número de expediente Qualcomm 121602P1) presentada el 15 de marzo de 2012. Además, el contenido de la solicitud no provisional con el número de expediente Qualcomm 113346 titulada: COMUNICACIÓN INALÁMBRICA UTILIZANDO CONFIGURACIÓN DE CONEXIÓN Y RE-AUTENTIFICACIÓN CONCURRENTE, presentada el 11 de septiembre de 2012, y la solicitud no provisional con el número de expediente Qualcomm 121602, titulada: SISTEMAS Y PROCEDIMIENTOS PARA CODIFICAR INTERCAMBIOS CON UN CONJUNTO DE DATOS DE CLAVE EFÍMERA COMPARTIDA, presentada el 11 de septiembre de 2012, son relevantes.

ANTECEDENTES

Campo

[0002] Lo siguiente se refiere en general a la comunicación inalámbrica y más específicamente a vincular los procesos de configuración y autentificación en la comunicación inalámbrica.

Descripción de la técnica relacionada

[0003] Los avances en la tecnología han dado lugar a dispositivos informáticos personales más pequeños y más potentes. Por ejemplo, existe actualmente una variedad de dispositivos informáticos personales portátiles, incluyendo dispositivos informáticos inalámbricos, tales como teléfonos inalámbricos portátiles, asistentes digitales personales (PDA) y dispositivos de búsqueda que son pequeños y ligeros y que pueden ser fácilmente transportados por los usuarios. Más específicamente, los teléfonos inalámbricos portátiles, tales como teléfonos celulares y teléfonos de protocolo de Internet (IP), pueden comunicar paquetes de voz y datos a través de redes inalámbricas. Además, muchos de tales teléfonos inalámbricos incluyen otros tipos de dispositivos que se incorporan en ellos. Por ejemplo, un teléfono inalámbrico también puede incluir una cámara digital, una cámara de vídeo digital, un grabador digital y un reproductor de archivos de audio. Además, dichos teléfonos inalámbricos pueden procesar instrucciones ejecutables, incluidas aplicaciones de software, como una aplicación de navegador de Internet, que se pueden utilizar para acceder a Internet. Como tales, estos teléfonos inalámbricos pueden incluir capacidades informáticas significativas.

[0004] Las redes de comunicación inalámbrica permiten a los dispositivos de comunicación transmitir y/o recibir información mientras está en movimiento. Estas redes de comunicación inalámbrica pueden estar comunicativamente acopladas a otras redes públicas o privadas para permitir la transferencia de información hacia y desde el terminal de acceso móvil. Dichas redes de comunicación incluyen típicamente una pluralidad de puntos de acceso (AP) que proporcionan enlaces de comunicación inalámbrica a terminales de acceso (por ejemplo, dispositivos de comunicación móvil, teléfonos móviles, terminales de usuario inalámbricos). Los puntos de acceso pueden ser estacionarios (por ejemplo, fijados al suelo) o móviles (por ejemplo, montados en vehículos, satélites, etc.) y posicionados para proporcionar una amplia área de cobertura a medida que el terminal de acceso se mueva dentro del área de cobertura.

[0005] Los dispositivos portátiles pueden configurarse para comunicar datos a través de estas redes inalámbricas. Por ejemplo, muchos dispositivos están configurados para funcionar de acuerdo con una especificación del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.11 que permite el intercambio inalámbrico de datos a través de un punto de acceso. En algunos sistemas de comunicación, cuando un terminal de acceso móvil se conecta a una red de comunicación a través de un punto de acceso, realiza autentificación de acceso a la red. Cada vez que un terminal de acceso móvil se conecta a un punto de acceso diferente, puede ser necesario repetir el proceso de autentificación. Sin embargo, repetir este proceso de autentificación puede introducir retrasos significativos en la configuración.

[0006] Muchos dispositivos de comunicación están configurados para realizar una configuración de enlace tanto en un paso inicial de conexión como en una o más pasos de reconexión. Los sistemas actuales asumen la clave pre-compartida para la asignación de direcciones AP-IP después de la autentificación para proteger las asignaciones de direcciones IP.

[0007] Si bien la utilización de múltiples mensajes comunicados entre dos o más puntos de procesamiento de mensajes en el sistema permite la configuración de enlace, es altamente deseable reducir el número de mensajes comunicados mientras se mantiene un nivel de autentificación requerido de la comunicación.

[0008] Por otra parte, un dispositivo de comunicación móvil puede escanear en busca de un punto de acceso cercano antes de que se pueda realizar la configuración de enlace. Este escaneo puede ser "pasivo" o "activo". En el escaneo "pasivo", el dispositivo puede escuchar la actividad del punto de acceso (por ejemplo, un mensaje de control). En el escaneo "activo", el dispositivo puede radiodifundir una consulta y luego esperar las respuestas de los puntos de acceso cercanos. Por lo tanto, el escaneo "pasivo" puede tardar mucho tiempo y el escaneo "activo" puede consumir tanto tiempo como energía en el dispositivo de comunicación móvil.

[0009] El documento XP017674098 divulga una re-autentificación rápida, en la que una solicitud de asociación se envía al menos parcialmente sin protección. ANonce está incluido en la respuesta de asociación.

[0010] La invención actual se define mediante la materia objeto de las reivindicaciones independientes. Se definen modos de realización preferidos mediante las reivindicaciones dependientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0011] Diversas características, naturaleza y ventajas pueden resultar evidentes a partir de la descripción detallada expuesta a continuación cuando se toma junto con los dibujos, en los que los mismos caracteres de referencia identifican los elementos similares correspondientes.

La FIG. 1 es un diagrama conceptual que ilustra un ejemplo de una red inalámbrica;

La FIG. 2 es un diagrama de bloques que ilustra un ejemplo de un dispositivo de usuario.

La FIG. 3 es un diagrama de flujo que ilustra la mensajería que puede realizarse en una configuración de conexión convencional.

La FIG. 4 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con uno o más aspectos de la presente divulgación.

La FIG. 5 es un diagrama de flujo que ilustra la mensajería que puede realizarse al realizar la configuración y autentificación del enlace.

La FIG. 6 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 7 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 8 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 9 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 10 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 11 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 12 es un diagrama de flujo que ilustra la mensajería que puede realizarse durante un protocolo de re-autentificación.

La FIG. 13 ilustra una jerarquía de claves que puede usarse para un protocolo de re-autentificación.

La FIG. 14 es un diagrama de flujo que muestra un proceso a modo de ejemplo para generar y agrupar una solicitud de re-autentificación y una solicitud de descubrimiento en una solicitud de asociación.

La FIG. 15 es un diagrama de flujo que muestra un proceso a modo de ejemplo que funciona en una estación base para recibir y extraer una solicitud de re-autentificación y un mensaje de capa superior de una solicitud de asociación enviada por una estación / terminal.

La FIG. 16 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 17 es un diagrama de flujo que muestra un proceso a modo de ejemplo que puede ser accionado en la estación de la FIG. 16 para realizar la configuración y autentificación del enlace.

La FIG. 18 es un diagrama de flujo que muestra un proceso a modo de ejemplo operable en el punto de acceso de la FIG. 16 para realizar la configuración y autentificación del enlace.

La FIG. 19 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 20 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace.

La FIG. 21 es un diagrama de flujo que muestra un proceso a modo de ejemplo operable en la estación de las FIGs. 19-20 para realizar la configuración y autentificación del enlace.

La FIG. 22 es un diagrama de flujo que muestra un proceso a modo de ejemplo operable en el punto de acceso de las FIGs. 19-20 para realizar la configuración y autentificación del enlace.

La FIG. 23 es un diagrama que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación de enlace.

La FIG. 24 es un diagrama de flujo que muestra un proceso a modo de ejemplo operable en una estación para realizar la configuración y autentificación de enlace como se muestra en la FIG. 23.

La FIG. 25 es un diagrama de flujo que muestra un proceso a modo de ejemplo operable en un punto de acceso para realizar la configuración y autentificación de enlace como se muestra en la FIG. 23.

La FIG. 26 es un diagrama que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación de enlace.

La FIG. 27 es un diagrama de flujo que muestra un proceso a modo de ejemplo operable en una estación para realizar la configuración y autentificación de enlace como se muestra en la FIG. 26.

La FIG. 28 es un diagrama de flujo que muestra un proceso a modo de ejemplo operable en un punto de acceso para realizar la configuración y autentificación de enlace como se muestra en la FIG. 26.

DESCRIPCIÓN DETALLADA

[0012] En la siguiente descripción, se hace referencia a los dibujos adjuntos, en los cuales se muestran, a modo de ilustración, modos de realización específicos en las que la divulgación puede ponerse en práctica. Los modos de realización pretenden describir aspectos de la divulgación con suficiente detalle para permitir que los expertos en la técnica practiquen la invención. A continuación, las partes de la descripción y los dibujos que se refieren a modos de realización que no están cubiertos por las reivindicaciones no deben entenderse como modos de realización de la invención, sino como antecedentes o ejemplos útiles para comprender la invención. El alcance de la invención se define solo mediante las reivindicaciones adjuntas.

[0013] Las características y aspectos descritos en el presente documento proporcionan dispositivos y procedimientos para un tiempo de configuración rápido durante un proceso de autentificación de una configuración de conexión. Por ejemplo, las técnicas descritas pueden permitir que un dispositivo móvil (por ejemplo, una estación (STA)) realice la configuración del enlace con respecto a un punto de acceso (AP) sin primero escuchar un baliza o solicitar una respuesta de sonda desde el punto de acceso. La respuesta de la sonda o la baliza puede incluir típicamente un punto de acceso creado para la ocasión (ANonce) que se utilizará durante la configuración del enlace. Por lo tanto, las técnicas descritas pueden permitir que la STA lleve a cabo la configuración del enlace sin haber recibido previamente el ANonce. De acuerdo con una técnica de "intercambio de 4 vías modificadas", la STA puede enviar una solicitud de asociación sin protección al AP y puede recibir el ANonce del AP en una respuesta de asociación. El ANonce recibido puede entonces ser utilizado para la obtención de clave. De acuerdo con una técnica de "ANonce siguiente", la STA puede recibir, durante una primera configuración de enlace iniciada usando un primer ANonce, un segundo ANonce para uso en una segunda configuración de enlace posterior a la primera configuración de enlace.

[0014] Las técnicas descritas también pueden permitir el uso de una clave temporal para la protección de la señalización de capa superior. Por ejemplo, en lugar de enviar una solicitud de asociación sin protección, una STA

puede recibir un primer ANonce (por ejemplo, ANonce1) a través de una baliza o una respuesta de sonda de un AP y puede obtener una primera clave (por ejemplo, una primera clave transitoria de pares (PTK)) basándose en el primer ANonce. La primera clave puede usarse para proteger la solicitud de asociación enviada por la STA al AP. En respuesta a la recepción de la solicitud de asociación, el AP puede generar un segundo ANonce (por ejemplo, ANonce2) y puede obtener una segunda clave (por ejemplo, una segunda PTK) basada en el segundo ANonce. El AP puede transmitir una respuesta de asociación a la STA que incluye el segundo ANonce y que está protegida usando la segunda clave. La STA puede obtener la segunda clave basada en el segundo ANonce y puede utilizar la segunda clave para procesar la respuesta de asociación y completar la configuración del enlace. La segunda clave también se puede usar para proteger los mensajes posteriores (por ejemplo, mensajes de datos) comunicados entre la STA y el AP.

[0015] De forma alternativa, en vez de recibir un ANonce desde el AP a través de una respuesta de la sonda o la baliza, la STA puede recibir una semilla de ANonce en la respuesta de la sonda o la baliza. La semilla de ANonce puede ser un valor de semilla criptográfica que es actualizado frecuentemente por el AP. La STA puede generar un ANonce recogiendo la semilla de ANonce con la dirección de control de acceso a medios (MAC) dirección de la STA. Por lo tanto, a diferencia de un ANonce que se radiodifunde a múltiples STAs a través de un mensaje de baliza, el ANonce generado en la STA basado en la semilla de ANonce y la dirección MAC de la STA pueden ser únicos para la STA. El ANonce generado puede ser utilizado por la STA para iniciar una configuración de enlace con el AP. Durante la configuración del enlace, el AP puede generar el ANonce basándose en la semilla de ANonce y la dirección MAC de la STA, que puede incluirse en los mensajes de configuración de enlace (por ejemplo, una solicitud de asociación) de la STA. Se observará que, en contraste con otras técnicas de intercambio, esta técnica puede implicar que la STA genere el ANonce antes que el AP. Ventajosamente, el ANonce puede ser exclusivo de la STA, puede enviarse "en claro" (es decir, sin cifrar) y puede no ser predecible mediante dispositivos no autorizados antes de la transmisión mediante el AP.

[0016] En un modo de realización particular, un procedimiento incluye enviar una solicitud de asociación sin protección desde un dispositivo móvil a un punto de acceso. El procedimiento también incluye recibir una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un ANonce. El procedimiento incluye la generación, en el dispositivo móvil, de una clave transitoria de pares (PTK) usando el ANonce.

[0017] En otro modo de realización particular, un aparato incluye un procesador y una memoria que almacena instrucciones ejecutables por el procesador para enviar una solicitud de asociación sin protección a un punto de acceso y para recibir una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un ANonce. Las instrucciones también son ejecutables por el procesador para generar una PTK usando el ANonce.

[0018] En otro modo de realización particular, un procedimiento incluye, en un punto de acceso, la recepción de una solicitud de asociación sin protección desde un dispositivo móvil. El procedimiento también incluye extraer un mensaje de inicio de la solicitud de asociación sin protección y enviar el mensaje de inicio a un servidor de autentificación. El procedimiento incluye además recibir un mensaje de respuesta desde el servidor de autentificación, donde el mensaje de respuesta incluye una clave de sesión principal de re-autentificación (rMSK). El procedimiento incluye generar un ANonce y enviar una respuesta de asociación al dispositivo móvil, donde la respuesta de asociación incluye el ANonce.

[0019] En otro modo de realización particular, un aparato incluye un procesador y una memoria que almacena instrucciones ejecutables por el procesador para recibir una solicitud de asociación sin protección desde un dispositivo móvil. Las instrucciones también son ejecutables por el procesador para extraer un mensaje de inicio de la solicitud de asociación sin protección y para enviar el mensaje de inicio a un servidor de autentificación. Las instrucciones son además ejecutables por el procesador para recibir un mensaje de respuesta desde el servidor de autentificación, donde el mensaje de respuesta incluye una rMSK. Las instrucciones son ejecutables por el procesador para generar un ANonce y para enviar una respuesta de asociación al dispositivo móvil, donde la respuesta de asociación incluye el ANonce.

[0020] En otro modo de realización particular, un procedimiento incluye iniciar, en un dispositivo móvil, una primera configuración de enlace con un punto de acceso utilizando un primer ANonce. El procedimiento también incluye recibir, durante la primera configuración de enlace con el punto de acceso, un segundo ANonce para uso en una segunda configuración de enlace con el punto de acceso posterior a la primera configuración de enlace, donde el segundo ANonce es distinto del primer ANonce.

[0021] En otro modo de realización particular, un aparato incluye un procesador y una memoria que almacena instrucciones ejecutables por el procesador para iniciar una primera configuración de enlace con un punto de acceso utilizando un primer ANonce. Las instrucciones son también ejecutables por el procesador para recibir, durante la primera configuración de enlace con el punto de acceso, un segundo ANonce para uso en una segunda configuración de enlace con el punto de acceso posterior a la primera configuración de enlace, donde el segundo ANonce es distinta del primer ANonce.

[0022] En otro modo de realización particular, un procedimiento incluye el envío, desde un punto de acceso a un dispositivo móvil durante una primera configuración de enlace que utiliza un primer ANonce, de un segundo ANonce para uso en una segunda configuración de enlace con el dispositivo móvil con posterioridad a la primera configuración de enlace, donde el segundo ANonce es distinto del primer ANonce.

[0023] En otro modo de realización particular, un aparato incluye un procesador y una memoria que almacena instrucciones ejecutables por el procesador para el envío, a un dispositivo móvil durante una primera configuración de enlace que utiliza un primer ANonce, de un segundo ANonce para uso en una segunda configuración de enlace con el dispositivo móvil con posterioridad a la primera configuración de enlace, donde el segundo ANonce es distinto del primer ANonce.

[0024] En otro modo de realización particular, un procedimiento incluye la recepción, en un dispositivo móvil, de un primer ANonce desde un punto de acceso. El procedimiento también incluye generar una primera PTK usando el primer ANonce. El procedimiento incluye además enviar una solicitud de asociación al punto de acceso, donde la solicitud de asociación incluye un SNonce y está protegida usando la primera PTK. El procedimiento incluye recibir una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un segundo ANonce y está protegida usando una segunda PTK. El procedimiento también incluye generar la segunda PTK usando el segundo ANonce y el SNonce. El procedimiento incluye además el uso de la segunda PTK para proteger al menos un mensaje posterior para enviarse al punto de acceso.

[0025] En otro modo de realización particular, un aparato incluye un procesador y una memoria que almacena instrucciones ejecutables por el procesador para generar, en un punto de acceso, una semilla de ANonce para enviarse a un dispositivo móvil. Las instrucciones son también ejecutables por el procesador para generar un ANonce basándose en la semilla de ANonce y una dirección MAC del dispositivo móvil que se recibe desde el dispositivo móvil. Las instrucciones son además ejecutables por el procesador para realizar una configuración de enlace con el dispositivo móvil basándose en el ANonce generado.

[0026] En las redes inalámbricas, tales como redes 802.11 (WiFi), un usuario móvil puede pasar de una red a otra. En algunos casos, las redes pueden ser gestionadas por una misma entidad o portadora de red.

[0027] Algunos ejemplos no limitantes de tales casos de uso son:

1. Paso por puntos de acceso

(A) Un usuario puede pasar por (varios, no superpuestos) puntos de acceso WiFi accesibles al público (por ejemplo, en cafeterías u otros lugares públicos). Mientras tiene conectividad, el terminal de usuario puede cargar y descargar información como mensajes de correo electrónico, mensajes de redes sociales, etc. Otro ejemplo son los pasajeros a bordo de un tren que puede pasar por múltiples estaciones de tren con puntos de acceso WiFi.

2. Tren

(B) Un usuario puede estar a bordo de un tren en el que se proporciona un servicio WiFi a los clientes a través de un punto de acceso local (AP). Este AP puede utilizar una red troncal inalámbrica basado en 802.11 para conectarse a la infraestructura al lado de las vías. Puede utilizarse una antena direccional para proporcionar una cobertura continua a lo largo de las vías

3. Paso por peaje / báscula

(C) Un vehículo en una carretera que pasa por un peaje o una báscula puede ser capaz de conectarse a un AP en el peaje o la báscula. Mientras se pasa por el peaje (o se realiza el pesaje), puede proporcionarse información tal como la facturación al cliente de peajes o intercambio de información de carga.

[0028] Las aplicaciones habilitadoras para estas conexiones no superpuestas pero relacionadas pueden basarse en un conjunto de protocolos de IP estándar y confiar potencialmente en la tecnología inalámbrica subyacente para establecer un enlace seguro.

[0029] En algunos sistemas propuestos para la configuración de conexiones de protocolo de Internet (IP), después de recibir una baliza, puede haber 16 intercambios de ida y vuelta (32 mensajes comunicados desde y hacia un terminal de acceso) para establecer un enlace seguro para el terminal de acceso.

[0030] En modos de realización seleccionados de sistemas propuestos descritos en el presente documento, se puede realizar una configuración de enlace rápido en la que el número de mensajes para configurar una conexión IP y enlace seguro después de recibir la baliza se reduce a 1 intercambio de ida y vuelta (2 mensajes) respecto a los 16 intercambios de ida y vuelta (32 mensajes) anteriores. Se puede utilizar un protocolo de autentificación extensible / protocolo de re-autentificación (EAP / ERP) como parte de la configuración de enlace rápido.

[0031] La FIG. 1 es un diagrama conceptual que ilustra un ejemplo de una configuración de red inalámbrica para comunicar datos entre uno o más terminales y un punto de acceso. La configuración de red 100 de la FIG. 1 puede utilizarse para comunicar datos entre uno o más terminales y un punto de acceso. La configuración de red 100 incluye un punto de acceso 102 acoplado a una red 104. El punto de acceso 102 puede estar configurado para proporcionar comunicaciones inalámbricas a diversos dispositivos de comunicación tales como dispositivos inalámbricos (que también pueden denominarse en el presente documento estaciones (STA) y terminales de acceso (AT) 106, 108, 110). Como ejemplo no limitativo, el punto de acceso 102 puede ser una estación base. Como ejemplos no limitativos, las estaciones / terminales 106, 108, 110 pueden ser un ordenador personal (PC), un ordenador portátil, una tableta, un teléfono móvil, un asistente digital personal (PDA), y/o cualquier dispositivo configurado para enviar y/o recibir datos de forma inalámbrica, o cualquier combinación de los mismos. La red 104 puede incluir una red de ordenadores distribuida, tal como una red de protocolo de control de transmisión / protocolo de Internet (TCP/IP).

[0032] El punto de acceso 102 puede estar configurado para proporcionar una variedad de servicios de comunicaciones inalámbricas, incluyendo, pero sin limitarse a: Servicios inalámbricos de fidelidad (WiFi), interoperabilidad mundial para servicios de acceso por microondas (WiMAX) y servicios de protocolo de iniciación de sesión inalámbrica (SIP). Las estaciones / terminales 106, 108, 110 pueden configurarse para comunicaciones inalámbricas (incluyendo, pero sin limitarse a, comunicaciones de acuerdo con la familia de especificaciones 802.11, 802.11-2007 y 802.11x desarrollada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)). Además, las estaciones / terminales 106, 108, 110 pueden configurarse para enviar datos y recibir datos desde el punto de acceso 102.

[0033] La FIG. 2 es un diagrama de bloques que ilustra un terminal / estación a modo de ejemplo 200. Un procesador 210 (por ejemplo, un Procesador de Señal Digital (DSP)) está acoplado a una memoria 232 para almacenar información tal como datos para procesamiento y transmisión e instrucciones 260 para su ejecución en el procesador 210. Las instrucciones pueden ser ejecutables por el procesador 210 para realizar diversos procedimientos y funciones de una estación / terminal, como se describe en el presente documento. Además, un punto de acceso (AP), un servidor de autentificación (AS), y un servidor de protocolo de configuración principal dinámica (DHCP) pueden incluir de manera similar un procesador y una memoria que almacena instrucciones ejecutables por el procesador para realizar varios procedimientos y funciones de un AP, AS y servidor DHCP, respectivamente, tal como se describe en el presente documento.

[0034] Un controlador de visualización 226 puede estar acoplado al procesador 210 y a un dispositivo de visualización 228. También se puede acoplar un codificador / descodificador (CÓDEC) 234 al procesador 210. Como ejemplos no limitativos de dispositivos de interfaz de usuario, un altavoz 236 y un micrófono 238 pueden estar acoplados al CÓDEC 234. Un controlador inalámbrico 240 puede estar acoplado al procesador 210 y a una antena 242. En un ejemplo particular, el procesador 210, el controlador de visualización 226, la memoria 232, el CÓDEC 234 y el controlador inalámbrico 240 pueden estar incluidos en un dispositivo de sistema en paquete o sistema en chip 222. En un ejemplo particular, un dispositivo de entrada 230 y una fuente de alimentación 244 pueden estar acoplados al dispositivo de sistema en chip 222. Además, en un ejemplo particular, como se ilustra, el dispositivo de visualización 228, el dispositivo de entrada 230, el altavoz 236, el micrófono 238, la antena 242 y el suministro de alimentación 244 pueden ser externos al dispositivo de sistema en chip 222. Sin embargo, cada uno del dispositivo de visualización 228, el dispositivo de entrada 230, el altavoz 236, el micrófono 238, la antena inalámbrica 242 y el suministro de alimentación 244 pueden acoplarse a un componente del dispositivo de sistema en chip 222, tal como una interfaz o un controlador.

[0035] La FIG. 3 es un diagrama de flujo que ilustra la mensajería que puede realizarse en una configuración de conexión convencional. Los mensajes mostrados entre la estación / terminal 302 y el punto de acceso 304 pueden incluir una sonda y solicitud de autentificación. Puede iniciarse un proceso de protocolo de autentificación extensible (EAP) sobre red local (LAN) (EAPOL) e incluir una fase de identificación, una fase EAP protegida (PEAP) y un protocolo de autentificación de intercambio de autentificación de EAP-Microsoft (EAP-MSCHAPv2). Después del éxito de EAP, se puede establecer una clave EAPOL. De este modo, al menos 16 mensajes deben ser comunicados a y desde la estación / terminal 302 para establecer la configuración y autentificación del enlace.

[0036] En modos de realización particulares del sistema propuesto descrito en el presente documento, el número de mensajes para configurar una conexión IP (después de la recepción de la baliza) se reduce a 2 mensajes (de 16 mensajes). El Protocolo de Re-autentificación del Protocolo de Autentificación Extensible (ERP) se puede utilizar como parte de la re-autentificación como se describe más completamente a continuación con respecto a las FIGS. 12 y 13 y pueden incluir las siguientes optimizaciones. La estación / terminal (STA) 302 puede realizar la autentificación completa de EAP una vez, y seguir usando la re-autentificación rápida de ERP para establecer una configuración de enlace inicial rápida a partir de entonces.

[0037] Una clave de sesión principal de re-autentificación (rMSK) es generada por la estación / terminal 302 antes de enviar una solicitud de asociación sin obtener una autentificación desde la red. La estación (STA) 302 de la rMSK genera una clave transitoria de pares (PTK) que incluye una clave de confirmación de clave (KCK), una clave de

cifrado de clave (KEK) y una clave transitoria (TK).

[0038] La solicitud de asociación es enviada por la estación 302 y agrupa una solicitud de re-autorización de EAP con un Protocolo de Configuración Principal Dinámica (DHCP) - Descubrimiento con Compromiso Rápido y un SNonce (por ejemplo, SNonce es recogido por la STA 302, es decir, estación creada para la ocasión). El mensaje agrupado puede incluirse como uno o más elementos de información (IEs). La solicitud de re-autorización de EAP es autentificada por el servidor de autentificación (servidor de aut.) 308 utilizando una clave de integridad de re-autentificación (rIK). El Descubrimiento con Compromiso Rápido de DHCP y SNonce se protegen mediante la clave de sesión principal de re-autentificación (rMSK) o la clave transitoria de pares (PTK) obtenida de la rMSK. El Descubrimiento con Compromiso Rápido de DHCP puede ser cifrado y MIC'd (Código de Integridad de Mensaje) o no cifrado pero MIC'd. Aunque algunos de los ejemplos del presente documento pueden utilizar una solicitud de descubrimiento (por ejemplo, Descubrimiento con Compromiso Rápido) para ilustrar un concepto de re-autentificación eficaz, debe entenderse que cualquier mensaje utilizado en una capa superior (de una pila de protocolos) para asignar la dirección IP puede ser utilizado en su lugar.

[0039] Si se cifra el mensaje DHCP, el punto de acceso 304 puede sostener los mensajes de Descubrimiento con Compromiso Rápido de DHCP y mensajes SNonce hasta que la solicitud de re-autentificación de EAP es validada por el servidor de autentificación 308. Para validar el mensaje, el punto de acceso (AP) 304 espera hasta que reciba una rMSK del servidor de autentificación 308 y obtenga la clave transitoria de pares (PTK). Basándose en la rMSK obtenida del servidor de autentificación 308, el punto de acceso 304 obtiene la PTK que se utiliza para MIC (Código de Integridad de Mensaje) así como para descifrar el mensaje.

[0040] Si el mensaje DHCP no está cifrado, el punto de acceso 304 puede reenviar el Descubrimiento con Compromiso Rápido de DHCP a un servidor DHCP con la expectativa de que la mayoría de los casos, el mensaje provino de un dispositivo correcto (pero conservar los mensajes SNonce hasta que la solicitud de re-autentificación de EAP sea validada por el servidor de autentificación 308). Aunque el Descubrimiento con Compromiso Rápido de DHCP puede ser enviado al servidor DHCP, el punto de acceso 304 mantendrá una confirmación de DHCP hasta que verifique el mensaje de descubrimiento de DHCP basándose en la rMSK obtenida del servidor de autentificación 308 y el punto de acceso 304 obtiene la PTK.

[0041] El punto de acceso (AP) 304 envía entonces la confirmación de DHCP + un GTK / IGTK protegido con la PTK. En otras palabras, la confirmación de DHCP está cifrado y la integridad del mensaje está protegida.

[0042] Un aspecto no limitativo puede incluir el uno o más de los siguientes pasos en un proceso para la autentificación y configuración de enlace.

[0043] En primer lugar, un usuario puede obtener una estación / terminal 302 y realizar una autentificación de EAP completa como parte de una configuración inicial con una red específica (por ejemplo, una red WiFi específica). Como ejemplo no limitativo, tal vez la autentificación de EAP completa pueda mantenerse durante un periodo de autentificación específico, tal como, por ejemplo, un año.

[0044] En segundo lugar, durante el periodo de autentificación, el usuario pasa por (varios, no superpuestos) puntos de acceso WiFi accesibles públicamente (por ejemplo, en cafeterías y otros lugares públicos). En otras palabras, este paso puede realizarse varias veces y con múltiples puntos de acceso 304 que forman parte de la red de configuración durante el periodo de autentificación. La estación / terminal 302 realizará una configuración de enlace inicial rápida (FILS) con la red utilizando ERP. La agrupación del ERP con el Descubrimiento Rápido de DHCP utilizando el mensaje de solicitud de asociación reducirá la señalización para la solicitud de asociación a una isa y vuelta, como se explica más detalladamente a continuación. Durante el periodo de autentificación, la estación / terminal de usuario 302 puede continuar realizando el ERP para la configuración de enlace inicial rápida (FILS) cuando se conecta con la red.

[0045] En tercer lugar, cuando se acerque el final de los periodos de autentificación, el usuario puede recibir una advertencia para realizar de nuevo un "acoplamiento completo" a la red, dentro de un periodo determinado de tiempo (por ejemplo, 2 semanas). Durante este periodo, el usuario seguirá siendo capaz de utilizar la autentificación rápida basada en la autentificación de EAP completa anterior hasta que expire o se realice un acoplamiento completo. La notificación de acoplamiento completo puede originarse desde la red o puede configurarse localmente en la estación / terminal 302.

[0046] En cuarto lugar, si el usuario no realiza el acoplamiento completo, después de un año, la red fallará a ERP e iniciará la autentificación completa de EAP durante otro año como se describe resumidamente en el paso 1.

[0047] Las FIGs. 4-11 ilustran varios escenarios diferentes para realizar la configuración y la autentificación del enlace de dos mensajes.

[0048] La FIG. 4 es un diagrama de flujo que ilustra un primer ejemplo de realización de una configuración y autentificación de enlace eficaces para una estación cliente. En los pasos 0a y 0b, mientras está comunicativamente

acoplada a un primer punto de acceso AP1 304A, la estación / terminal (STA) 302 puede realizar la autentificación de EAP completa. Al moverse (paso 1) más cerca de un segundo punto de acceso AP2 304B, y detectar su baliza (paso 2), la estación / terminal 302 puede intentar re-autentificarse por medio del segundo punto de acceso AP2 304B. En este proceso, el punto de acceso 304B transmite una baliza / sonda que incluye un indicador de capacidad para la configuración de enlace inicial rápida (FILS). El indicador de capacidad puede indicar la capacidad de manejar una solicitud de asociación con Descubrimiento Rápido de DHCP y ERP agrupado En el paso 3, la estación / terminal 302 genera unas claves de sesión principales de re-autentificación (rMSK) (véase la FIG. 13) utilizando ERP antes de enviar la solicitud de asociación, donde:

rMSK = KDF (K, S);
K = rRK; y
S = rMSK etiqueta | "\ 0" | SEQ | longitud.

[0049] La estación / terminal 302 agrupa los uno o más mensajes como elementos de información (IEs) (o parámetros / carga útil) de una solicitud de asociación (Paso 3). Por ejemplo, tal solicitud de asociación puede incluir: 1) Iniciar la autentificación de EAP (integridad de mensaje usando rIK); 2) Descubrimiento de DHCP con Compromiso Rápido (cifrado e integridad de mensajes con KCK / KEK); y/o 3) Clave EAPOL (SNonce, ANonce) (integridad del mensaje usando KCK). La clave EAPOL puede configurarse como una trama o subconjunto completo. El ANonce (es decir, el punto de acceso creado para la ocasión) puede ser seleccionado por la estación / terminal 302 y enviado al punto de acceso AP2 304B. El punto de acceso (AP2) 304B puede asegurar que la estación / terminal 302 está usando un ANonce enviado en los últimos segundos / milisegundos (por ejemplo, un ANonce reciente obtenido de la baliza para el AP2), por ejemplo. El punto de acceso AP2 304B contiene el mensaje de clave DHCP y EAPOL hasta que recibe una clave de sesión principal original (rMSK) del servidor de autentificación 308. El punto de acceso AP2 304B genera una PTK desde la rMSK. El punto de acceso AP2 304B realiza un intercambio de Código de Integridad de Mensaje (MIC) para los mensajes de clave DHCP y EAPOL y descifra el DHCP. El punto de acceso AP2 304B utiliza la rMSK para obtener KCK / KEK para proteger una confirmación de DHCP y un mensaje de clave EAPOL antes de enviarlo a la estación / terminal 302.

[0050] En diversos ejemplos, el ANonce puede ser enviado por el AP2 304B ya sea usando la baliza para permitir que las estaciones que utilizan escaneo pasivo, o en un mensaje de respuesta de sonda cuando se usa el escaneo activo. Cuando el ANonce es enviado por el AP2 304B usando la baliza, el ANonce se puede cambiar en cada baliza, o un múltiplo de balizas. La estación 302 puede incluir el ANonce escogido por la estación 302 en el mensaje de Solicitud de Asociación enviado desde la estación 302 a AP2 304B.

[0051] La FIG. 5 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Este proceso puede denominarse Opción 1a. Los procesos realizados en la FIG. 5 son similares a los realizados en la FIG. 4 (Opción 1), excepto que se utiliza la rMSK (en lugar de la KCK / KEK de la PTK) para autentificar los mensajes de descubrimiento de DHCP y clave EAPOL encapsulados en el mensaje de solicitud de asociación.

[0052] La FIG. 6 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Este proceso puede denominarse Opción 1b. Los procesos realizados en la FIG. 6 son similares a los realizados en la FIG. 4 (Opción 1), excepto las siguientes diferencias posibles. El paso 2 mostrado en la FIG. 6, el punto de acceso 304 puede anunciar una capacidad de que la solicitud de DHCP pueda cifrarse. El paso 4 mostrado en la FIG. 6, la estación / terminal 302 puede decidir si el mensaje DHCP debe ser cifrado o no. Varios factores pueden ser tomados en consideración por la estación / terminal 302, tales como, por ejemplo, si la solicitud de descubrimiento de DHCP contiene cualquier información privada, etc. Si la estación / terminal decide cifrar la solicitud de descubrimiento de DHCP, entonces el punto de acceso 304 puede contener el mensaje (como se muestra en las FIGs. 4 y 5).

[0053] Si la estación / terminal decide no cifrar la solicitud de Descubrimiento de DHCPr, se pueden realizar los siguientes pasos. El paso 4 mostrado en la FIG. 6, el elemento de información (IE) de solicitud de descubrimiento de DHCP o el parámetro solo está protegido contra la integridad de mensajes. Basándose en el paso 4, el punto de acceso 304 envía el Descubrimiento con Compromiso Rápido de DHCP (paso 6) sin esperar una respuesta para una solicitud de inicio de re-autentificación de EAP (paso 9). Este proceso hace que la asignación de direcciones IP tenga lugar en paralelo con el procedimiento de re-autentificación de EAP. En el paso 7a mostrado en la FIG. 6, el punto de acceso contiene la confirmación de DHCP que provenía del servidor DHCP hasta el paso 10b, en la que se ha validado el Descubrimiento de DHCP. Si la integridad del mensaje falla, entonces el punto de acceso 304 inicia un procedimiento para eliminar la dirección IP asignada mediante la confirmación de DHCP.

[0054] La FIG. 7 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Este proceso puede denominarse Opción 2. Los procesos realizados en la FIG. 7 son similares a los realizados en la FIG. 4 (Opción 1), excepto las siguientes diferencias posibles. En lugar de autentificar el mensaje DHCP y el mensaje de clave EAPOL de forma independiente, la carga útil combinada que incluye la re-autentificación de EAP, el Descubrimiento de DHCP y la clave EAPOL puede autentificarse utilizando KCK / KEK. El punto de acceso 304 extrae el mensaje de inicio de re-autentificación de EAP

y lo envía al servidor de autentificación 308 sin validar el mensaje completo, que se autentificó utilizando KCK / KEK. El punto de acceso 304 autentifica el mensaje completo después de recibir la Rmsk del servidor de autentificación 308.

[0055] La FIG. 8 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Este proceso puede denominarse Opción 2a. Los procesos realizados en la FIG. 8 son similares a los realizados en la FIG. 5 (Opción 1a), salvo las siguientes posibles diferencias. En lugar de autentificar el mensaje DHCP y el mensaje de clave EAPOL de forma independiente, la carga útil combinada que incluye la re-autentificación de EAP, el descubrimiento de DHCP y la clave EAPOL pueden autentificarse utilizando la rMSK. El punto de acceso 304 extrae el mensaje de inicio de re-autentificación de EAP y lo envía al servidor de autentificación 308 sin validar el mensaje completo, que se autentificó utilizando la rMSK. El punto de acceso 304 autentifica el mensaje completo después de recibir la rMSK del servidor de autentificación 308. El mensaje de descubrimiento de DHCP (paso 9) se puede enviar antes del paso 5. En este caso, la dirección IP asignada se omite si la autentificación no tiene éxito.

[0056] La FIG. 9 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Este proceso puede denominarse Opción 2b. Los procesos realizados en la FIG. 9 son similares a los realizados en la FIG. 4 excepto por las siguientes diferencias posibles. En el paso 2, el punto de acceso puede anunciar la capacidad de que la solicitud DHCP puede cifrarse. En el paso 4, la estación / terminal 302 decide si el mensaje DHCP debe estar cifrado o no. Varios factores pueden ser tomados en consideración por la estación / terminal 302, tales como, por ejemplo, si la solicitud de descubrimiento de DHCP contiene cualquier información privada, etc. Si la estación / terminal 302 decide cifrar la solicitud de descubrimiento de DHCP, entonces el punto de acceso 304 mantendrá el mensaje como se ha descrito anteriormente en la opción 2 y en la opción 2a. Si la estación / terminal 302 decide no cifrar la solicitud de descubrimiento de DHCP, entonces se pueden realizar los siguientes pasos. En el paso 4, el mensaje de descubrimiento de DHCP IE solo está protegido contra la integridad del mensaje. Basándose en el paso 4, el punto de acceso 304 envía el Descubrimiento con Compromiso Rápido de DHCP (paso 6) sin esperar respuesta para la Solicitud de Inicio de Re-autentificación de EAP (paso 9). Este proceso hace que la asignación de direcciones IP tenga lugar en paralelo con el procedimiento de re-autentificación de EAP. En el paso 7a, el punto de acceso 304 contiene la confirmación de DHCP que provenía del servidor DHCP hasta el paso 10b, en el que se ha validado el descubrimiento de DHCP. Si falla la integridad del mensaje, entonces el punto de acceso 304 inicia un procedimiento para eliminar la dirección IP asignada mediante el mensaje de confirmación de DHCP.

[0057] La FIG. 10 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Este proceso puede denominarse Opción 3. Los procesos realizados en la FIG. 10 son similares a los realizados en las FIGs. 4 y 5 (Opciones 1 y 1a), salvo las siguientes diferencias posibles. El ANonce se puede enviar en la respuesta de asociación junto con un mensaje "Instalar PTK, GTK, IGTK". Los pasos 9 y 11 en la FIG. 10 puede realizarse en paralelo con los pasos 5 - 7 como se describe en la opción 1b y la opción 2b.

[0058] Una opción 4 también se puede obtener a partir de las opciones 1 y 2, excepto por las siguientes diferencias posibles. En lugar de un solo mensaje en el paso 4 (es decir, la solicitud de asociación), la solicitud de asociación puede dividirse como mensaje 1 (M1), que encapsula el mensaje de descubrimiento de DHCP y el mensaje 2 (M2), que encapsula el mensaje de inicio de re-autentificación de EAP y el SNonce. El punto de acceso 304 no actuará sobre el mensaje de descubrimiento de DHCP hasta que reciba la clave EAPOL. Los dos mensajes (M1 y M2) pueden estar separados por un periodo SIFS. Esta opción 4 puede tener una ventaja de que la estructura EAPOL puede ser reutilizada.

[0059] La FIG. 11 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Este proceso puede denominarse Opción 5. Los procesos realizados en la FIG. 11 son similares a los realizados en la FIG. 4 (Opción 1), excepto las siguientes diferencias posibles. El punto de acceso 304 transmite la respuesta de sonda / baliza, que incluye el indicador de capacidad de Ajuste de Enlace Inicial Rápido (FILS) para la asignación simultánea de direcciones ERP y/o IP. En este escenario, el temporizador de arrendamiento de la dirección IP asignada por el punto de acceso 304 no ha expirado. La estación / terminal 302 usa la dirección IP asignada por un primer punto de acceso 304A en una solicitud DHCP enviada a un segundo punto de acceso 304 para confirmar si puede continuar usando esa dirección IP. Si la dirección IP ha expirado, entonces el servidor DHCP 306 envía un DHCP-NAK.

[0060] La FIG. 12 es un diagrama de flujo que ilustra la mensajería que puede realizarse durante un protocolo de re-autentificación. La primera vez que la estación / terminal 302 se conecta a una red, realiza un intercambio de EAP completo con el servidor de autentificación 308. Como resultado, una clave de sesión principal (MSK) se distribuye al autentificador de EAP. La clave de sesión principal (MSK) es entonces utilizada por el autentificador y la estación / terminal 302 para establecer claves de sesión transitorias (TSK) según sea necesario. En el momento del intercambio inicial de EAP, la estación / terminal 302 y el servidor de autentificación 308 también obtienen una EMSK, que se utiliza para obtener una clave original de re-autentificación (rRK). Más específicamente, una clave original de re-autentificación (rRK) puede obtenerse a partir de la MSK ampliada (EMSK) o de una clave original

específica del dominio (DSRK), que se obtiene a partir de la EMSK. La clave original de re-autentificación (rRK) puede estar solamente disponible para la estación / terminal 302 y el servidor de autentificación 308 y en general no se distribuye a ninguna otra entidad. Además, una clave de integridad de re-autentificación (rIK) puede obtenerse a partir de la clave original de re-autentificación (rRK). La estación / terminal 302 y el servidor de autentificación 308 pueden usar la clave de integridad de re-autentificación (rIK) para proporcionar prueba de posesión mientras se realiza un intercambio de ERP. La clave de integridad de re-autentificación (rIK) también en general no se distribuye a ninguna otra entidad y en general solo está disponible para la estación / terminal 302 y el servidor de autentificación 308.

[0061] Dos nuevos códigos de EAP, Inicio de EAP y Finalización de EAP, se definen con el fin de re-autentificación de EAP. Cuando la estación / terminal 302 solicita un ERP, realiza el intercambio de ERP mostrado en la ventana inferior de la FIG. 12.

[0062] La FIG. 13 ilustra una jerarquía de claves que puede usarse para un protocolo de re-autentificación. La clave de sesión principal (MSK) se puede obtener a partir de una clave original y una clave principal de pares (PMK) se puede obtener a partir de la clave de sesión principal (MSK). La MSK ampliada (EMSK) puede obtenerse a partir de la clave original. Para el intercambio de ERP, se pueden obtener varias claves adicionales de la MSK ampliada (EMSK). Se puede obtener DSRK1-DSRKn. Cada una de las claves de clave original específica del dominio (DSRK) puede incluir el rRK. A partir de la clave original de re-autentificación (rRK), se puede obtener la clave de integridad de re-autentificación (rIK) y las claves de sesión principal de re-autentificación (rMSK1 ... rMSKn). Cada una de las rMSK puede incluir una clave principal de pares (PMK). Se puede obtener a partir de la PMK una clave transitoria de pares (PTK) (que puede incluir una clave de confirmación de clave (KCK), una clave de cifrado de clave (KEK) y una clave transitoria (TK)).

[0063] La FIG. 14 es un diagrama de flujo que muestra un proceso a modo de ejemplo 1400 que funciona en una estación / terminal para generar y agrupar una solicitud de re-autentificación y un mensaje de la capa superior (por ejemplo, solicitud de descubrimiento) en una solicitud de asociación. El bloque de funcionamiento 1402 indica que se recibe desde el punto de acceso una baliza que incluye un número aleatorio o creado para la ocasión (por ejemplo, ANonce). En el bloque de funcionamiento 1404, el terminal genera una solicitud de re-autentificación con un protocolo de autentificación extensible a partir de una clave de cifrado utilizando el número aleatorio o creado para la ocasión. En el bloque de funcionamiento 1406, el terminal genera un mensaje de capa superior. Por ejemplo, dicho mensaje de capa superior puede ser una solicitud de descubrimiento, una solicitud de descubrimiento con compromiso rápido de protocolo de configuración principal dinámica (DHCP)
y/o el mensaje de asignación de direcciones del protocolo de Internet (IP).

[0064] El bloque de funcionamiento 1408 indica que, en algunos aspectos, el terminal puede generar una clave de sesión principal de re-autentificación (rMSK) que responde a los resultados de un proceso de autentificación anterior. El bloque de operaciones 1410 indica que en algunos aspectos el terminal puede generar una clave transitoria de pares (PTK) a partir de la rMSK, el número aleatorio (ANonce) y/o un número aleatorio generado localmente (SNonce).

[0065] El bloque de funcionamiento 1412 indica que en algunos aspectos el terminal puede cifrar el mensaje de la capa superior con la rMSK. El bloque de funcionamiento 1414 indica que en algunos aspectos el terminal puede cifrar el mensaje de capa superior con la PTK o una combinación de la KCK y la KEK. En otros aspectos, el mensaje de la capa superior puede no estar cifrado.

[0066] El bloque de funcionamiento 1416 indica que en algunos aspectos el terminal puede generar la solicitud de asociación como un primer mensaje que encapsula un mensaje de descubrimiento de DHCP, un segundo mensaje que encapsula un mensaje de inicio de re-autentificación de EAPOL.

[0067] El bloque de funcionamiento 1418 indica que el terminal agrupa el mensaje de la capa superior y la solicitud re-autentificación como una solicitud de asociación. El bloque de funcionamiento 1420 indica que en algunos aspectos el terminal puede transmitir el primer mensaje y el segundo mensaje por separado.

[0068] La FIG. 15 es un diagrama de flujo que muestra un proceso a modo de ejemplo 1500 que funciona en una estación base para recibir y extraer una solicitud de re-autentificación y un mensaje de la capa superior de una solicitud de asociación enviada por una estación / terminal. El bloque de funcionamiento 1502 indica que en algunos aspectos el punto de acceso puede generar un número aleatorio y transmitir una baliza que incluye el número aleatorio.

[0069] El bloque de funcionamiento 1504 indica que el punto de acceso recibe desde un terminal una solicitud de asociación que incluye un mensaje de capa superior (por ejemplo, solicitud de descubrimiento) y una solicitud de re-autentificación agrupados. El bloque de funcionamiento 1506 indica que el punto de acceso extrae el mensaje de capa superior de la solicitud de asociación y lo reenvía a un servidor de configuración. El bloque de funcionamiento 1508 indica que el punto de acceso extrae la solicitud de re-autentificación de la solicitud de asociación y la reenvía a un servidor de autentificación.

[0070] El bloque de funcionamiento 1510 indica que en algunos aspectos el punto de acceso puede recibir una clave de cifrado del servidor de autentificación. El bloque de funcionamiento 1512 indica que en algunos aspectos el punto de acceso puede generar una PTK desde la clave de cifrado, el número aleatorio y un número aleatorio recibido desde el terminal. El bloque de funcionamiento 1514 indica que en algunos aspectos el punto de acceso puede verificar el mensaje de capa superior con una combinación de KCK y KEK dentro de la PTK, lo cual incluye una clave de confirmación de clave de protocolo de autentificación extensible sobre LAN (EAPOL) y la clave de cifrado de clave (KEK) EAPOL.

[0071] Se observará que los modos de realización particulares descritos con referencia a las FIGs. 4-15 puede implicar un intercambio de 4 vías para la configuración de enlace inicial rápida. En general, el intercambio de 4 vías puede incluir: 1) El AP envía un ANonce a la STA, 2) la STA envía un SNonce al AP, 3) el AP envía una PTK a la STA, y 4) la STA confirma la finalización del intercambio.

[0072] Así, la primera parte del intercambio de 4 vías puede implicar una STA que escucha una baliza o solicita una respuesta de sonda a partir de un punto de acceso antes de iniciar la configuración de enlace con el punto de acceso. Por ejemplo, la respuesta de la sonda o la baliza puede incluir el ANonce que será utilizado por la STA para fines de cifrado y/o integridad del mensaje. Sin embargo, escuchar una baliza puede consumir tiempo y solicitar una respuesta de sonda puede consumir tiempo y energía. Por lo tanto, el tiempo y la energía en la STA pueden conservarse permitiendo que la STA lleve a cabo la configuración del enlace sin primero escuchar un baliza o solicitar una respuesta de sonda desde el punto de acceso.

[0073] La FIG. 16 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. En particular, la FIG. 16 ilustra un intercambio modificado de 4 vías que permite la configuración del enlace sin escuchar primero una baliza o solicitar una respuesta de sonda desde un punto de acceso.

[0074] Los mensajes y operaciones seleccionados ilustrados en la FIG. 16 pueden corresponder a los mensajes y operaciones ilustrados en las FIGs. 4-11, con las siguientes modificaciones. La STA 302 puede generar una rMSK y un SNonce, en el paso 2, y enviar una solicitud de asociación sin protección al AP 304, en el paso 3. La solicitud de asociación sin protección puede incluir el SNonce. En contraste con el modo de realización de la FIG. 4, la STA 302 puede realizar estas operaciones antes de recibir el ANonce y obtener la PTK. Debido a que la STA 302 envía la solicitud de asociación antes de recibir el ANonce y obtener la PTK, el AP 304 puede extraer y reenviar la porción de inicio de re-autentificación de EAP de la solicitud de asociación al AS 308, como se indica en el paso 4, sin realizar verificación de ANonce como se describe en la FIG. 4. En su lugar, el AP 304 puede confiar en que el AS 308 transmita un mensaje de respuesta con una rMSK obtenida (paso 7) como autentificación para la STA 302.

[0075] Después de recibir la rMSK, el AP 304 puede generar el ANonce, en el paso 9, y obtener la PTK basándose en el ANonce, la rMSK, y el SNonce, en el paso 10a. De este modo, la PTK puede obtenerse en el AP 304 antes de obtenerse en la STA 302. El AP 304 puede enviar una respuesta de asociación que incluye el ANonce a la STA 302, en el paso 12, donde la respuesta de asociación está protegida usando la KCK y KEK de la PTK. Después de recibir la respuesta de asociación del AP 304, la STA 302 puede generar la PTK utilizando la rMSK, el SNonce y el ANonce en la respuesta de asociación, en el paso 12a.

[0076] La respuesta de asociación enviada desde el AP 304 (que incluye el ANonce), está protegida por integridad usando el ANonce. Los elementos de información que no sean ANonce en la respuesta de asociación también pueden ser cifrados. De este modo, el AP 304 puede "pre-proteger" (es decir, pre-cifrar / pre-proteger con integridad) la respuesta de asociación usando una PTK generada en el AP 304 usando el SNonce obtenido de la STA 302 en la solicitud de asociación, una rMSK obtenida del AS 308, y el ANonce generado localmente que todavía no se ha transmitido a la STA 302. Al recibir la respuesta de asociación, la STA 302 extrae el ANonce de la respuesta de asociación, genera la PTK y verifica la protección de integridad del mensaje. Así, la STA 302 "post-valida" el mensaje basándose en una clave obtenida del mensaje. Tal pre-protección y post-validación puede permitir una configuración de enlace más rápida que los esquemas de intercambio convencionales que primero confirman las claves y luego protegen los datos usando las teclas.

[0077] El modo de realización de la FIG. 16 puede permitir así a la STA 302 realizar un intercambio modificado de 4 vías para la configuración del enlace sin primero escuchar un baliza o solicitar una respuesta de sonda. Esto puede reducir el tiempo de configuración del enlace y ahorrar energía en la STA 302. Debe tenerse en cuenta que debido a que la STA 302 no espera una respuesta de sonda / baliza, la STA 302 puede usar un mecanismo de direccionamiento alternativo para la solicitud de asociación sin protección. Por ejemplo, cuando el AP 304 es "conocido" para la STA 302, la STA 302 puede haber almacenado previamente un identificador de conjunto de servicios básicos (BSSID) del AP 304 en una memoria de la STA 302. Para iniciar la configuración del enlace, la STA 302 puede recuperar el BSSID almacenado y puede enviar la solicitud de asociación sin protección al AP 304 basándose en el BSSID. Las situaciones en las que el AP 304 puede ser "conocido" para la STA 302 incluyen cuando el AP 304 ha sido previamente visitado por la STA 302 (por ejemplo, un AP "de hogar" o un AP de "oficina") y cuando la STA 302 no se ha movido recientemente (por ejemplo, según lo determinado por una capacidad del

sistema de posicionamiento celular y/o global (GPS) de la STA 302). Por lo tanto, en un modo de realización particular, la STA 302 puede enviar la solicitud de asociación en respuesta a la información de localización determinada en la STA 302 (por ejemplo, cuando la STA 302 "sabe" que el AP 304 de destino está en la proximidad de la STA 302).

[0078] La FIG. 17 es un diagrama de flujo que muestra un proceso a modo de ejemplo 1700 operable en la STA 302 de la FIG. 16 para realizar la configuración y autentificación del enlace. En 1702, un dispositivo móvil (por ejemplo, la STA 302) puede recuperar un BSSID de un punto de acceso previamente visitado por el dispositivo móvil. Procediendo a 1704, el dispositivo móvil puede generar una rMSK y un SNonce. Avanzando hasta 1706, el dispositivo móvil puede enviar una solicitud de asociación sin protección al punto de acceso basándose en el BSSID. Por ejemplo, haciendo referencia a la FIG. 16, la STA 302 puede enviar la solicitud de asociación sin protección al AP 304 en el paso 3.

[0079] Continuando con 1708, el dispositivo móvil puede recibir una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un ANonce. En 1710, el dispositivo móvil puede generar una PTK usando la rMSK, el SNonce y el ANonce en la respuesta de asociación recibida. Por ejemplo, haciendo referencia a la FIG. 16, la STA 302 puede recibir la respuesta de asociación del AP 304 en el paso 12 y puede obtener la PTK en el paso 12a.

[0080] La FIG. 18 es un diagrama de flujo que muestra un proceso inventivo 1800 operable en el AP 304 de la FIG. 16 para realizar la configuración y autentificación del enlace. En 1802, un punto de acceso recibe una solicitud de asociación sin protección desde un dispositivo móvil, donde la solicitud de asociación sin protección incluye un SNonce. Procediendo a 1804, el punto de acceso extrae un mensaje de inicio de la solicitud de asociación sin protección. Continuando con 1806, el punto de acceso envía el mensaje de inicio a un servidor de autentificación y recibe un mensaje de respuesta desde el servidor de autentificación, donde el mensaje de respuesta incluye una rMSK. Por ejemplo, haciendo referencia a la FIG. 16, el AP 304 puede recibir la solicitud de asociación sin protección desde la STA 302 en el paso 3 y puede recibir la rMSK del AS 308 en el paso 8.

[0081] Avanzando hasta 1808, el punto de acceso puede generar un ANonce. El punto de acceso genera también una PTK utilizando la rMSK, el ANonce y el SNonce, en 1810. Continuando con 1812, el punto de acceso envía una respuesta de asociación al dispositivo móvil, donde la respuesta de asociación incluye el ANonce y está protegida usando la PTK. Por ejemplo, haciendo referencia a la FIG. 16, el AP 304 puede generar el ANonce en el paso 9, obtener la PTK en el paso 10a y enviar la respuesta de asociación a la STA 302 en el paso 12.

[0082] La FIG. 19 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. En particular, la FIG. 19 ilustra la provisión, durante una primera configuración de enlace, de un ANonce "siguiente" que se puede usar durante una segunda configuración de enlace posterior a la primera configuración de enlace.

[0083] Los mensajes y operaciones seleccionados ilustrados en la FIG. 16 pueden corresponder a los mensajes y operaciones ilustrados en las FIGs. 4-11, con las siguientes modificaciones. La STA 302 puede iniciar una primera configuración de enlace 1902 con el AP 304 usando un primer ANonce (por ejemplo, ANonce[x]). En un modo de realización particular, el primer ANonce puede haber sido previamente enviado por el AP 304 y recibido por la STA 302 a través de una respuesta de la sonda o la baliza (por ejemplo, como se muestra en el paso 2a), recuperado de una memoria de la STA 302 (por ejemplo, como se muestra en el paso 2b), o cualquier combinación de los mismos.

[0084] Durante la primera configuración de enlace 1902, la STA 302 puede transmitir una solicitud de asociación al AP 304 utilizando el primer ANonce (por ejemplo, ANonce[x]). El AP 304 puede proporcionar un segundo ANonce (por ejemplo, ANonce[x+1]) a la STA 302 durante la primera configuración de enlace 1902. El segundo ANonce puede ser para su uso en una segunda configuración de enlace posterior 1904 con el AP 304. Por ejemplo, el segundo ANonce puede proporcionarse en una respuesta de asociación (por ejemplo, como se muestra en el paso 4a), en un mensaje EAPOL (por ejemplo, como se muestra en el paso 4b), o en cualquier combinación de los mismos.

[0085] Cuando la STA 302 inicia la segunda configuración de enlace 1904 con el AP 304, la STA 302 puede utilizar el segundo ANonce (por ejemplo, ANonce[x+1]) en lugar de esperar una baliza o solicitar una respuesta de la sonda. En un modo de realización particular, el segundo ANonce (por ejemplo, ANonce[x+1] puede tener una duración de validez establecida por el AP 304, y la STA 302 puede determinar que el segundo ANonce es válido, en el paso 5a, antes de iniciar la segunda configuración de enlace 1904. Si se determina que el segundo ANonce no es válido, la STA 302 puede proceder como se describe con referencia a la FIG. 20.

[0086] Tras determinar que el segundo ANonce (por ejemplo, ANonce[x+1]) es válido, la STA puede iniciar la segunda configuración de enlace 1904 usando el segundo ANonce. Durante la segunda configuración de enlace 1904, la STA 302 puede enviar una segunda solicitud de asociación utilizando el segundo ANonce, como se muestra en el paso 6. La STA 302 también puede recibir un tercer ANonce (por ejemplo, ANonce[x+2]), para ser utilizado en una tercera configuración de enlace posterior con el AP 304, como se muestra en el paso 7a o 7b.

[0087] La FIG. 20 es un diagrama de flujo que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación del enlace. Los mensajes y operaciones ilustrados en la FIG. 20 pueden corresponder a los mostrados en la FIG. 19 con las siguientes modificaciones.

[0088] En el paso 5a, la STA 302 puede determinar que el segundo ANonce (por ejemplo, ANonce[x+1]) no es válido (por ejemplo, debido a la expiración de un periodo de tiempo de validez). De este modo, en lugar de poder utilizar el segundo ANonce durante la segunda configuración de enlace 1904, la STA 302 puede esperar o solicitar un nuevo ANonce (por ejemplo, ANonce[y]) a través de una respuesta de sonda o baliza, como se muestra en el paso 5b. El nuevo ANonce puede utilizarse entonces para iniciar la segunda configuración de enlace 1904. Durante la segunda configuración de enlace 1904, la STA 302 puede recibir desde el AP 304 otro ANonce (por ejemplo, ANonce[y+1]) para su uso en una tercera configuración de enlace posterior.

[0089] De este modo, los modos de realización descritos en las Figuras 19-20 pueden proporcionar un "próximo ANonce" a dispositivos móviles, de manera que una configuración de enlace posterior puede realizarse más rápidamente y puede consumir menos energía. Además, debe observarse que para facilitar la ilustración, los modos de realización de las FIGs. 19-20 pueden no incluir todos los mensajes implicados en la configuración del enlace. Por ejemplo, no se muestra la mensajería relacionada con las operaciones DHCP y la mensajería entre el AP 304 y el AS 308.

[0090] La FIG. 21 es un diagrama de flujo que muestra un proceso a modo de ejemplo 2100 operable en la STA 302 de las FIGs. 19-20 para realizar la configuración y autentificación del enlace. En 2102, un dispositivo móvil puede iniciar una primera configuración de enlace con un punto de acceso utilizando un primer ANonce. El primer ANonce puede ser recuperado de una memoria y/o recibido desde el punto de acceso a través de una baliza o una respuesta de sonda. Avanzando hasta 2104, el dispositivo móvil puede recibir, durante la primera configuración de enlace con el punto de acceso, un segundo ANonce para uso en una segunda configuración de enlace posterior con el punto de acceso. El segundo ANonce se puede recibir en una respuesta de asociación y/o un mensaje EAPOL. Por ejemplo, haciendo referencia a las FIGs. 19-20, la STA 302 puede iniciar la primera configuración de enlace 1902 utilizando el primer ANonce (por ejemplo, ANonce[x]) y puede recibir el segundo ANonce (por ejemplo, ANonce[x+1]) durante la primera configuración de enlace 1902.

[0091] Continuando con 2106, el dispositivo móvil puede determinar si el segundo ANonce es válido. Por ejemplo, el dispositivo móvil puede realizar dicha determinación antes de iniciar la segunda configuración de enlace. Con fines ilustrativos, el dispositivo móvil puede utilizar un temporizador que se envía junto con el segundo ANonce o un temporizador pre-configurado para determinar si el segundo ANonce es válido. Cuando se determina que el segundo ANonce es válido, el dispositivo móvil puede iniciar la segunda configuración de enlace utilizando el segundo ANonce, en 2108. Por ejemplo, haciendo referencia a la FIG. 19, la STA 302 puede iniciar la segunda configuración de enlace 1904 usando el segundo ANonce (por ejemplo, ANonce[x+1]).

[0092] Cuando el segundo ANonce se determina que no es válido, el dispositivo móvil puede recibir un nuevo ANonce del punto de acceso, en 2110. El ANonce nuevo puede ser recibido en una baliza o una respuesta de la sonda. Procediendo a 2112, el dispositivo móvil puede iniciar una configuración de enlace con el punto de acceso utilizando el nuevo ANonce. Por ejemplo, haciendo referencia a la FIG. 20, el dispositivo móvil puede usar el nuevo ANonce (por ejemplo, ANonce[y]) para la configuración del enlace.

[0093] La FIG. 22 es un diagrama de flujo que muestra un proceso a modo de ejemplo 2200 operable en el AP 304 de las FIGs. 19-20 para realizar la configuración y autentificación del enlace. En 2202, un punto de acceso puede enviar un primer ANonce a un dispositivo móvil. El primer ANonce se puede enviar antes de iniciar una primera configuración de enlace que utiliza el primer ANonce. Avanzando hasta 2204, el punto de acceso puede enviar al dispositivo móvil, durante la primera configuración de enlace, un segundo ANonce para su uso en una segunda configuración de enlace posterior con el dispositivo móvil. Por ejemplo, haciendo referencia a las FIGs. 19-20, durante la primera configuración de enlace 1902 que utiliza el primer ANonce (por ejemplo, ANonce[x]), el AP 304 puede enviar a la STA 302 el segundo ANonce (por ejemplo, ANonce[x+1]) para su uso en la configuración del segundo enlace posterior 1904.

[0094] La FIG. 23 es un diagrama que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación de enlace. En particular, la FIG. 23 ilustra el uso de una clave "temporal" (por ejemplo, PTK) para la protección de señalización de la capa superior durante la configuración del enlace. Dado que los mensajes de señalización de la capa superior tienen protección de seguridad incorporada (entre la STA 302 y el servidor de autentificación 308), los mensajes de señalización de la capa superior pueden protegerse usando un ANonce "más débil" (por ejemplo, un ANonce que tiene propiedades de seguridad más bajas), que puede permitir un procedimiento de señalización más rápido para la asociación. Un ANonce "más fuerte" se obtiene en paralelo a la señalización de la capa superior y se utiliza para la transferencia de datos adicional, como se describe en el presente documento.

[0095] Los mensajes y operaciones seleccionados ilustrados en la FIG. 23 puede corresponder al mensaje y las

operaciones ilustrados en las FIGs. 4-11, con las siguientes modificaciones. El AP 304 puede enviar un primer ANonce (por ejemplo, ANonce1) a la STA 302, como se muestra en el paso 2. La STA 302 puede obtener una primera PTK (por ejemplo, PTK1) basándose en ANonce1 y el SNonce de la STA 302, como se muestra en el paso 3a. En el paso 4, la STA 302 puede enviar una solicitud de asociación al AP 304. La solicitud de asociación puede incluir el SNonce y puede protegerse usando PTK1. Con fines ilustrativos, la solicitud de asociación puede protegerse usando una primera clave de confirmación de clave (KCK1) obtenida a partir de PTK1.

[0096] En el paso 8a, el AP 304 puede obtener PTK1 basándose en ANonce1 y el SNonce incluido en la solicitud de asociación. En el paso 12, el AP puede generar un segundo ANonce (por ejemplo, ANonce2) y puede obtener una segunda PTK (por ejemplo, PTK2) basándose en ANonce2 y SNonce. En el paso 13, el AP 304 puede enviar una respuesta de asociación a la STA 302, donde la respuesta de asociación incluye ANonce2 y está protegida usando PTK2. Con fines ilustrativos, la respuesta de asociación se puede proteger usando una KCK y una clave de cifrado de clave (KEK) obtenida basándose en PTK2. La STA 302 puede generar PTK2, en el paso 14, basándose en el SNonce y ANonce2 para completar la configuración del enlace. La PTK2 puede ser utilizada por la STA 302 y el AP 304 para proteger mensajes posteriores (por ejemplo, mensajes de datos) comunicados entre la STA 302 y el AP 304.

[0097] Por lo tanto, a diferencia del flujo de mensajes ilustrado en la FIG. 16, que implica la transmisión de una solicitud de asociación sin protección, el flujo de mensajes de la FIG. 23 protege la solicitud de asociación mediante una PTK1 "temporal". Se observará que aunque la PTK1 se genera usando un ANonce que puede ser conocido para múltiples STAs (por ejemplo, ANonce1 puede ser radiodifundido a múltiples STAs a través de una baliza), solo un mensaje (la solicitud de asociación) está protegido usando la clave "temporal" PTK1. Los mensajes posteriores, incluyendo la respuesta de asociación y los mensajes de datos entre la STA 302 y el AP 304, están protegidos usando una tecla diferente PTK2. El flujo de mensajes de la FIG. 23 puede de este modo ser preferible en situaciones en las que el AP no es "conocido" o "de confianza", tal como en las zonas de acceso público.

[0098] La FIG. 24 es un diagrama de flujo que muestra un proceso a modo de ejemplo 2400 operable en una estación, tal como la STA 302 que comunica y procesa mensajes como se ilustra en la FIG. 23, para realizar la configuración y autentificación del enlace. En 2402, un dispositivo móvil (por ejemplo, la STA 302) puede recibir un primer ANonce (por ejemplo, ANonce1) desde un punto de acceso (por ejemplo, el AP 304). Avanzando hasta 2404, el dispositivo móvil puede generar una primera PTK (por ejemplo, PTK1) usando el primer ANonce. Continuando con 2406, el dispositivo móvil puede enviar una solicitud de asociación al punto de acceso. La solicitud de asociación puede incluir un SNonce y puede protegerse usando la primera PTK.

[0099] En 2408, el dispositivo móvil puede recibir una respuesta de asociación desde el punto de acceso. La respuesta de asociación puede incluir un segundo ANonce (por ejemplo, ANonce2) y puede protegerse usando una segunda PTK (por ejemplo, PTK2). Avanzando hasta 2410, el dispositivo móvil puede generar la segunda PTK usando el segundo ANonce y el SNonce. Continuando con 2412, el dispositivo móvil puede usar la segunda PTK para proteger uno o más mensajes posteriores que se enviarán al punto de acceso.

[0100] La FIG. 25 es un diagrama de flujo que muestra un proceso a modo de ejemplo 2500 operable en un punto de acceso, tal como el AP 304 que comunica y procesa mensajes como se ilustra en la FIG. 23, para realizar la configuración y autentificación del enlace. En 2502, un punto de acceso (por ejemplo, el AP 304) puede enviar un primer ANonce (por ejemplo, ANonce1) a un dispositivo móvil (por ejemplo, la STA 302). Por ejemplo, el primer ANonce puede enviarse a través de una respuesta de sonda de unidifusión o una baliza de radiodifusión. Avanzando hasta 2504, el punto de acceso puede recibir una solicitud de asociación desde el dispositivo móvil. La solicitud de asociación puede incluir un SNonce y puede protegerse usando una primera PTK (por ejemplo, PTK1). En 2506, el punto de acceso puede generar la primera PTK basándose en el primer ANonce y el SNonce.

[0101] Continuando con 2508, el punto de acceso puede generar un segundo ANonce (por ejemplo, ANonce2) y una segunda PTK (por ejemplo, PTK2) basándose en el segundo ANonce y el SNonce. En 2510, el punto de acceso puede enviar una respuesta de asociación al dispositivo móvil. La respuesta de asociación puede incluir el segundo ANonce y puede protegerse usando la segunda PTK.

[0102] La FIG. 26 es un diagrama que ilustra la mensajería que puede realizarse de acuerdo con otros aspectos de la configuración y autentificación de enlace. En particular, la FIG. 26 ilustra el uso de una semilla de ANonce para generar un ANonce.

[0103] Los mensajes y operaciones seleccionados ilustrados en la FIG. 26 pueden corresponder a los mensajes y operaciones ilustrados en las FIGs. 4-11, con las siguientes modificaciones. El AP 304 puede enviar una semilla de ANonce a la STA 302 en una respuesta de la sonda o la baliza, como se muestra en el paso 2. En un modo de realización particular, la semilla de ANonce es un valor de semilla criptográfica de 64 bits que se actualiza con frecuencia mediante el AP 304. En un modo de realización particular, la semilla de ANonce se radiodifunde a una pluralidad de STA (por ejemplo, en una baliza). La STA 302 puede utilizar la semilla de ANonce para generar un dispositivo ANonce específico, como se muestra en el paso 3. En un modo de realización particular, el ANonce se genera realizando una función (por ejemplo, una función de recogida) en la semilla de ANonce y un valor único y/o

descriptivo de la STA 302 (por ejemplo, una dirección MAC de la STA 302 o algún otro valor asociado con la STA 302). Se apreciará que a diferencia de un ANonce radiodifundido a múltiples STAs, el ANonce generado en el paso 3 puede ser exclusivo de la STA 302. La STA 302 puede realizar una configuración de enlace con el AP 304 basándose en el ANonce generado.

[0104] En el paso 8a, el AP 304 puede obtener el ANonce basándose en la semilla de ANonce y la dirección MAC de la STA 302. Por ejemplo, la dirección MAC de la STA 302 puede ser recuperada por el AP 304 a partir de la respuesta de asociación enviada en el paso 4. El AP 304 puede realizar y completar la configuración del enlace con la STA 302 después de generar el ANonce.

[0105] Se observará que a diferencia de otras técnicas de recogida, el modo de realización de la FIG. 26 implica que la STA 302 genere el ANonce antes del AP 304. Sin embargo, para preservar la compatibilidad hacia atrás, el ANonce generado de acuerdo con las técnicas de semilla de ANonce de la FIG. 26 pueden compartir propiedades similares a ANonces en técnicas de intercambio. Por ejemplo, el ANonce puede ser exclusivo para la STA 302, el ANonce y/o semilla de ANonce puede enviarse "en el claro" (por ejemplo, utilizando un mensaje de baliza o respuesta de sonda como se muestra en el paso 2 o un mensaje de clave EAPOL como se muestra en el paso 4), y el ANonce puede no ser predecible mediante dispositivos no autorizados antes de la transmisión mediante el AP 304.

[0106] La FIG. 27 es un diagrama de flujo que muestra un proceso a modo de ejemplo 2700 operable en una estación, tal como la STA 302 que comunica y procesa mensajes como se ilustra en la FIG. 26, para realizar la configuración y autentificación del enlace. En 2702, un dispositivo móvil (por ejemplo, la STA 302) puede recibir una semilla de ANonce desde un punto de acceso (por ejemplo, el AP 304). Avanzando hasta 2704, el dispositivo móvil puede generar un ANonce basándose en la semilla de ANonce y una dirección MAC del dispositivo móvil. Continuando con 2706, el dispositivo móvil puede realizar una configuración de enlace con el punto de acceso basándose en el ANonce generado.

[0107] La FIG. 28 es un diagrama de flujo que muestra un proceso a modo de ejemplo 2800 operable en un punto de acceso, tal como el AP 304 que comunica y procesa mensajes como se ilustra en la FIG. 26, para realizar la configuración y autentificación del enlace. En 2802, un punto de acceso (por ejemplo, el AP 304) puede enviar una semilla de ANonce a un dispositivo móvil (por ejemplo, la STA 302). Avanzando hasta 2804, el punto de acceso puede recibir una dirección MAC del dispositivo móvil. Por ejemplo, la dirección MAC puede incluirse en un mensaje desde el dispositivo móvil, tal como una solicitud de asociación. Continuando con 2806, el punto de acceso puede generar un ANonce basado en la semilla de ANonce y la dirección MAC del dispositivo móvil. En 2808, el punto de acceso puede verificar la autenticidad del dispositivo móvil comparando el ANonce comunicado por el dispositivo móvil con el ANonce calculado por el punto de acceso. Si el dispositivo móvil pasa la verificación, entonces el punto de acceso puede realizar una configuración de enlace con el dispositivo móvil basándose en el ANonce generado.

[0108] Hay que señalar que aunque pueden describirse diversos modos de realización y opciones en el presente documento como alternativas, se pueden combinar diferentes características de diferentes modos de realización y opciones para realizar la autentificación de una configuración de enlace.

[0109] Diversas técnicas descritas en el presente documento pueden aplicarse a escenarios de datos de extracción e introducción. Por ejemplo, el intercambio de 4 vías modificado descrito con referencia a las FIGs. 16-18 y la "siguiente" técnica ANonce descrita con referencia a las FIGs. 19-22 pueden aplicarse a los escenarios de datos basados en extracción e interacción Una o más aplicaciones ejecutadas por un dispositivo móvil, como correo electrónico y aplicaciones de redes sociales, pueden verificar periódicamente actualizaciones de datos. El intercambio de 4 vías modificado o la "siguiente" técnica de ANonce puede permitir que la extracción de actualizaciones de dichos datos se produzca más rápido y con un consumo de batería reducido en el dispositivo móvil. Como otro ejemplo, la(s) aplicación(es) en el dispositivo móvil puede(n) estar configurada(s) para recibir actualizaciones de datos introducidas (por ejemplo, desde servidores). Una porción inicial de una actualización de datos puede recibirse por una conexión celular. Sin embargo, el resto de la actualización de datos se puede recibir más rápido (por ejemplo, por WiFi) y/o con un consumo de batería reducido porque la porción inicial de la actualización de datos activa una configuración de enlace inicial rápida utilizando el intercambio de 4 vías modificado o la "siguiente" técnica de ANonce como se describe en el presente documento. La técnica PTK temporal descrita con referencia a las FIGs. 23-25 y la técnica de semilla de ANonce descrita con referencia a las FIGs. 26-28 también se pueden usar en estos escenarios de datos basados en extracción e introducción.

[0110] En conjunción con los modos de realización descritos, un primer aparato puede incluir medios para enviar una solicitud de asociación sin protección desde un dispositivo móvil a un punto de acceso. Por ejemplo, los medios de envío pueden incluir uno o más componentes de las STA 106-110, el controlador inalámbrico 240, la antena 242, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para enviar una solicitud de asociación sin protección, o cualquier combinación de los mismos. El primer aparato puede incluir también medios para recibir una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un ANonce. Por ejemplo, los medios para recibir pueden incluir uno o más componentes de las STA 106-110, el controlador inalámbrico 240, la antena 242, uno o más componentes de la STA 302, uno o más dispositivos

diferentes configurados para recibir una respuesta de asociación, o cualquier combinación de los mismos. El primer aparato puede incluir además medios para generar, en el dispositivo móvil, una PTK usando el ANonce. Por ejemplo, los medios para generar pueden incluir uno o más componentes de las STA 106-110, el procesador 210, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para generar una PTK, o cualquier combinación de los mismos.

[0111] Un segundo aparato puede incluir medios para recibir una solicitud de asociación sin protección en un punto de acceso desde un dispositivo móvil. Por ejemplo, los medios para recibir la solicitud de asociación sin protección pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para recibir una solicitud de asociación sin protección (por ejemplo, un controlador inalámbrico y/o antena de un AP), o cualquier combinación de los mismos. El segundo aparato puede incluir también medios para extraer un mensaje de inicio de la solicitud de asociación sin protección. Por ejemplo, los medios para extraer pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para extraer un mensaje de inicio (por ejemplo, un procesador de un AP), o cualquier combinación de los mismos. El segundo aparato puede incluir además medios para enviar el mensaje de inicio a un AS. Por ejemplo, los medios para enviar el mensaje de inicio pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para enviar un mensaje de inicio (por ejemplo, un controlador inalámbrico y/o antena de un AP), o cualquier combinación de los mismos.

[0112] El segundo aparato puede incluir medios para recibir un mensaje de respuesta desde el AS, en el que el mensaje de respuesta incluye una rMSK. Por ejemplo, los medios para recibir el mensaje de respuesta pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para recibir un mensaje de respuesta (por ejemplo, un controlador inalámbrico y/o Antena de un AP), o cualquier combinación de los mismos. El segundo aparato puede incluir también medios para generar un ANonce. Por ejemplo, los medios para generar pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para generar un ANonce (por ejemplo, un procesador de un AP), o cualquier combinación de los mismos. El segundo aparato puede incluir además medios para enviar una respuesta de asociación desde el punto de acceso al dispositivo móvil, donde la respuesta de asociación incluye el ANonce. Por ejemplo, los medios para enviar la respuesta de asociación pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para enviar una respuesta de asociación (por ejemplo, un controlador inalámbrico y/o Antena de un AP), o cualquier combinación de los mismos.

[0113] Un tercer aparato puede incluir medios para iniciar, en un dispositivo móvil, una primera configuración de enlace con un punto de acceso utilizando un primer ANonce. Por ejemplo, los medios para iniciar pueden incluir uno o más componentes de las STA 106-110, el procesador 210, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para iniciar una configuración de enlace, o cualquier combinación de los mismos. El tercer aparato puede incluir también medios para recibir, durante la primera configuración de enlace con el punto de acceso, un segundo ANonce para uso en una segunda configuración de enlace con el punto de acceso posterior a la primera configuración de enlace. Por ejemplo, los medios para recibir pueden incluir uno o más componentes de las STA 106-110, el controlador inalámbrico 240, la antena 242, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para recibir un ANonce, o Cualquier combinación de los mismos.

[0114] Un cuarto aparato puede incluir medios para enviar, desde un punto de acceso a un dispositivo móvil durante una primera configuración de enlace que utiliza un primer ANonce, un segundo ANonce para uso en una segunda configuración de enlace con el dispositivo móvil posterior a la primera configuración de enlace. Por ejemplo, los medios para enviar el segundo ANonce pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para enviar un ANonce (por ejemplo, un controlador inalámbrico y/o una antena De un AP), o cualquier combinación de los mismos. El cuarto aparato puede incluir también medios para enviar el primer ANonce al dispositivo móvil a través de una baliza o una respuesta de sonda antes del inicio de la primera configuración de enlace, donde el segundo ANonce es distinto del primer ANonce. Por ejemplo, los medios para enviar el primer ANonce pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para enviar un ANonce (por ejemplo, un controlador inalámbrico y/o una antena de un AP), o cualquier combinación de los mismos.

[0115] Un quinto aparato puede incluir medios para recibir, en un dispositivo móvil, un primer ANonce desde un punto de acceso. Por ejemplo, los medios para recibir pueden incluir uno o más componentes de las STA 106-110, el controlador inalámbrico 240, la antena 242, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para recibir un ANonce, o Cualquier combinación de los mismos. El aparato también puede incluir medios para generar una primera PTK usando el primer ANonce. Por ejemplo, los medios para generar pueden incluir uno o más componentes de las STA 106-110, el procesador 210, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para generar una PTK, o cualquier combinación de los mismos. El primer ANonce puede considerarse un ANonce "débil", por ejemplo debido a que se radiodifunde a múltiples STAs en una baliza o debido a que tiene un valor predecible. Sin embargo, el uso de un ANonce "débil" tal vez sea

aceptable debido a la seguridad implícita incorporada en mensajes de señalización de capa superior. Además, se puede obtener un segundo ANonce "más fuerte" y utilizarse para una transferencia de datos adicional, como se describe en el presente documento.

[0116] El aparato puede incluir además medios para enviar una solicitud de asociación al punto de acceso, donde la solicitud de asociación incluye un SNonce y se protege usando la primera PTK. Por ejemplo, los medios para enviar pueden incluir uno o más componentes de las STA 106-110, el controlador inalámbrico 240, la antena 242, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para enviar una solicitud de asociación, o cualquier combinación de los mismos.

[0117] El aparato puede incluir medios para recibir, en el dispositivo móvil, una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un segundo ANonce y se protege usando una segunda PTK. Por ejemplo, los medios para recibir pueden incluir uno o más componentes de las STA 106-110, el controlador inalámbrico 240, la antena 242, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para recibir una respuesta de asociación, o cualquier combinación de los mismos. El segundo ANonce puede considerarse un ANonce "fuerte".

[0118] El aparato puede incluir también medios para generar, en el dispositivo móvil, la segunda PTK usando el segundo ANonce y el SNonce. Por ejemplo, los medios para generar pueden incluir uno o más componentes de las STA 106-110, el procesador 210, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para generar una PTK, o cualquier combinación de los mismos. El aparato puede incluir además medios para utilizar la segunda PTK para proteger al menos un mensaje posterior para ser enviado desde el dispositivo móvil al punto de acceso. Por ejemplo, los medios de uso pueden incluir uno o más componentes de las STA 106-110, el procesador 210, uno o más componentes de la STA 302, uno o más dispositivos diferntes configurados para proteger un mensaje, o cualquier combinación de los mismos.

[0119] Un sexto aparato puede incluir medios para enviar, desde un punto de acceso, un primer ANonce a un dispositivo móvil. Por ejemplo, los medios de envío pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para enviar un ANonce, o cualquier combinación de los mismos. El aparato también puede incluir medios para recibir una solicitud de asociación desde el dispositivo móvil, donde la solicitud de asociación incluye un SNonce y está protegida usando una primera PTK. Por ejemplo, los medios para recibir pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para recibir una solicitud de asociación, o cualquier combinación de los mismos.

[0120] El aparato puede incluir además medios para generar, en el punto de acceso, la primera PTK basándose en el primer ANonce y el SNonce. Por ejemplo, los medios para generar pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para generar una PTK, o cualquier combinación de los mismos. El aparato puede incluir medios para generar un segundo ANonce. Por ejemplo, los medios para generar un segundo ANonce pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para generar un ANonce, o cualquier combinación de los mismos. El aparato también puede incluir medios para generar una segunda PTK basándose en el segundo ANonce y el SNonce. Por ejemplo, los medios para generar pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para generar una PTK, o cualquier combinación de los mismos.

[0121] El aparato puede incluir además medios para enviar una respuesta de asociación al dispositivo móvil, donde la respuesta de asociación incluye el segundo ANonce y está protegida usando la segunda PTK. Por ejemplo, los medios para enviar pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para enviar una respuesta de asociación, o cualquier combinación de los mismos.

[0122] Un séptimo aparato puede incluir medios para recibir, en un dispositivo móvil, una semilla de ANonce a partir de un punto de acceso. La semilla de ANonce se puede radiodifundir a una pluralidad de dispositivos (por ejemplo, a través de una baliza). Por ejemplo, los medios para recibir una semilla de ANonce pueden incluir uno o más componentes de las STA 106-110, el controlador inalámbrico 240, la antena 242, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para recibir una semilla de ANonce, o cualquier combinación de los mismos. El aparato también puede incluir medios para generar, en el dispositivo móvil, un ANonce basándose en la semilla de ANonce y una dirección MAC del dispositivo móvil. Por ejemplo, los medios para generar pueden incluir uno o más componentes de las STA 106-110, el procesador 210, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para generar un ANonce, o cualquier combinación de los mismos.

[0123] El aparato puede incluir además medios para realizar una configuración de enlace con el punto de acceso basándose en el ANonce generado. Por ejemplo, los medios para realizar pueden incluir uno o más componentes de las STA 106-110, el procesador 210, uno o más componentes de la STA 302, uno o más dispositivos diferentes configurados para realizar una configuración de enlace, o cualquier combinación de los mismos.

[0124] Un octavo aparato puede incluir medios para enviar, desde un punto de acceso, una semilla de ANonce a un dispositivo móvil. Por ejemplo, los medios para enviar pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para enviar una semilla de ANonce, o cualquier combinación de los mismos.

[0125] El aparato también puede incluir medios para recibir una dirección MAC del dispositivo móvil. Por ejemplo, los medios para recibir pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para recibir una dirección MAC, o cualquier combinación de los mismos. El aparato puede incluir además medios para generar un ANonce basándose en la semilla de ANonce y la dirección MAC del dispositivo móvil. Por ejemplo, los medios para generar pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para generar un ANonce, o cualquier combinación de los mismos.

[0126] El aparato puede incluir medios para realizar una configuración de enlace con el dispositivo móvil basándose en el ANonce generado. Por ejemplo, los medios para realizar pueden incluir uno o más componentes del AP 102, uno o más componentes del AP 304, uno o más dispositivos diferentes configurados para realizar una configuración de enlace, o cualquier combinación de los mismos.

[0127] La anterior descripción de los modos de realización divulgados se proporciona para permitir que cualquier experto en la técnica realice o use los modos de realización divulgados. Diversas modificaciones de estos modos de realización resultarán fácilmente evidentes a los expertos en la técnica, y los principios definidos en el presente documento pueden aplicarse a otros modos de realización sin apartarse del alcance de la divulgación. Por lo tanto, la presente divulgación no pretende limitarse a los modos de realización divulgados en el presente documento, sino que se le concede el alcance más amplio posible compatible con los principios y características novedosas definidos en las reivindicaciones siguientes.

[0128] Los elementos descritos en el presente documento pueden incluir múltiples instancias del mismo elemento. Estos elementos pueden ser indicados genéricamente por un designador numérico (por ejemplo, 110) e indicados específicamente por el indicador numérico seguido de un designador alfabético (por ejemplo, 110A) o un indicador numérico precedido de un "guion" (por ejemplo, 110-1). Para facilitar el seguimiento de la descripción, la mayor parte de los indicadores de número de elemento empiezan con el número del dibujo en el que se introducen o describen los elementos con mayor detalle.

[0129] Debería entenderse que cualquier referencia a un elemento del presente documento que use una designación tal como "primer", "segundo", y así sucesivamente, no limita la cantidad o el orden de esos elementos, a no ser que dicha limitación esté indicada explícitamente.. En su lugar, estas designaciones pueden usarse en el presente documento como un procedimiento conveniente para distinguir entre dos o más elementos o ejemplos de un elemento. Por lo tanto, una referencia a un primer y segundo elementos no significa que puedan usarse solamente dos elementos o que el primer elemento deba preceder al segundo elemento de alguna forma. Además, a menos que se indique de otra forma, un conjunto de elementos puede comprender uno o más elementos.

[0130] Las implementaciones específicas mostradas y descritas son solo ejemplos y no deben interpretarse como la única manera de implementar la presente divulgación a menos que se especifique lo contrario en el presente documento. Es fácilmente evidente para un experto en la técnica que los diversos ejemplos en la presente divulgación pueden ser practicados por numerosos sistemas de partición diferentes.

[0131] Los expertos en la técnica entenderán que la información y las señales pueden representarse usando cualquiera entre varias tecnologías y técnicas diferentes. Por ejemplo, los datos, las instrucciones, los comandos, la información, las señales, los bits, los símbolos y los chips que pueden haberse mencionado a lo largo de esta descripción pueden representarse mediante tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos o cualquier combinación de estos. Algunos dibujos pueden ilustrar señales como una sola señal para claridad de presentación y descripción. Un experto en la técnica entenderá que la señal puede representar un bus de señales, en el que el bus puede tener una variedad de anchos de bits y la presente divulgación puede implementarse en cualquier número de señales de datos, incluyendo una única señal de datos.

[0132] En la descripción, elementos, circuitos y funciones pueden mostrarse en forma de diagrama de bloques con el fin de no oscurecer la presente divulgación con detalles innecesarios. A la inversa, las implementaciones específicas mostradas y descritas son solamente ilustrativas y no deben interpretarse como la única manera de implementar la presente divulgación a menos que se especifique lo contrario en el presente documento. Además, las definiciones de bloques y el particionamiento de la lógica entre varios bloques es un ejemplo de una implementación específica. Es fácilmente evidente para un experto en la técnica que la presente divulgación puede ser practicada por numerosos otros sistemas de partición. En su mayor parte, se han omitido los detalles relativos a las consideraciones de temporización y similares, cuando tales detalles no son necesarios para obtener una comprensión completa de la presente divulgación y están dentro de las capacidades de personas con conocimientos ordinarios en la técnica pertinente.

[0133] Uno o más de los componentes, actos, características y/o funciones descritos en el presente documento e ilustrados en los dibujos pueden reorganizarse y/o combinarse en un único componente, acto, característica, o función o incorporados en varios componentes, actos, características o funciones. También pueden añadirse elementos, componentes, actos y/o funciones adicionales sin apartarse de la invención. Los algoritmos descritos en el presente documento también pueden implementarse eficientemente en software y/o integrarse en hardware.

[0134] Además, debe observarse que los modos de realización pueden describirse como un proceso que se representa como un organigrama, un diagrama de flujo, un diagrama estructural o un diagrama de bloques. Aunque un diagrama de flujo puede describir las operaciones como un proceso secuencial, muchas de las operaciones pueden realizarse en paralelo o simultáneamente. Además, el orden de las operaciones puede reorganizarse. Un proceso se termina cuando sus operaciones se completan. Un proceso puede corresponder a un procedimiento, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un proceso se corresponde con una función, su finalización corresponde al retorno de la función a la función de llamada o la función principal.

[0135] Además, un medio de almacenamiento puede representar uno o más dispositivos para almacenar datos, incluyendo memora de solo lectura (ROM), memoria de acceso aleatorio (RAM), medios de almacenamiento de disco magnético, medios de almacenamiento óptico, dispositivos de memoria flash y/u otros medios legibles por máquina y medios legibles por procesador y/o medios legibles por ordenador para almacenar información. Las expresiones "medio legible a máquina", "medio legible por ordenador", y/o "medio legible por procesador" pueden incluir, pero sin limitación, medios no transitorios como dispositivos de almacenamiento fijos o portátiles, dispositivos de almacenamiento ópticos, y otros medios diferentes capaces de almacenar, contener o transportar instrucciones y/o datos. Por lo tanto, los diversos procedimientos descritos en el presente documento pueden implementarse parcial o completamente mediante instrucciones y/o datos que pueden almacenarse en un "medio legible por máquina", "medio legible por ordenador", y/o un "medio legible por procesador" y ejecutarse mediante uno o más procesadores, máquinas y/o dispositivos.

[0136] Además, los modos de realización pueden implementarse mediante hardware, software, firmware, middleware, microcódigo, o cualquier combinación de los mismos. Al implementarse en software, firmware, middleware o microcódigo, el código de programa o segmentos de código para realizar las tareas necesarias pueden almacenarse en un medio legible por máquina, tal como un medio de almacenamiento u otro almacenamiento o almacenamientos. Un procesador puede realizar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o sentencias de programa. Un segmento de código puede acoplarse a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. La información, argumentos, parámetros, datos, etc. se puede pasar, enviar o transmitir a través de un medio adecuado que incluye compartir la memoria, el paso de mensajes, el paso de testigos, transmisión por red, etc.

[0137] Los diversos bloques lógicos, módulos, circuitos, elementos y/o componentes ilustrativos descritos en relación con los ejemplos divulgados en el presente documento pueden implementarse o realizarse con un procesador de uso general, con un procesador de señales digitales (DSP), con un circuito integrado de aplicación específica (ASIC), con una matriz de puertas de campo programable (FPGA) o con otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos, o con cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de uso general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de componentes informáticos, por ejemplo una combinación de un DSP y un microprocesador, varios microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo. Un procesador de uso general, configurado para ejecutar los modos de realización descritos en el presente documento, se considera un procesador de uso especial para llevar a cabo dichos modos de realización. De forma similar, un ordenador de uso general se considera un ordenador de uso especial cuando está configurado para llevar a cabo los modos de realización descritos en el presente documento.

[0138] Los procedimientos o algoritmos descritos en relación con los ejemplos divulgados en el presente documento pueden incorporarse directamente en hardware, en un módulo de software ejecutable por un procesador, o en una combinación de ambos, en forma de unidad de procesamiento, instrucciones de programación, u otras direcciones, y pueden contenerse en un único dispositivo o distribuirse a través de múltiples dispositivos. Un módulo de software puede residir en memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, registros, un disco duro, un disco extraíble, un CD-ROM o en cualquier otra forma de medio de almacenamiento conocida en la técnica. Un medio de almacenamiento puede estar acoplado al procesador de manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador.

[0139] Por ejemplo, la funcionalidad STA pueden implementarse utilizando instrucciones almacenadas en un medio legible por procesador. Un medio particular puede almacenar instrucciones ejecutables para hacer que un

procesador genere una solicitud de asociación sin protección para ser enviada por un dispositivo móvil a un punto de acceso. Las instrucciones también pueden ser ejecutables para hacer que el procesador genere una PTK usando un ANonce recuperado de una respuesta de asociación desde el punto de acceso. Otro medio particular puede almacenar instrucciones ejecutables por un procesador para iniciar, en un dispositivo móvil, una primera configuración de enlace con un punto de acceso utilizando un primer ANonce. Las instrucciones también pueden ser ejecutables para hacer que el procesador reciba, durante la primera configuración de enlace con el punto de acceso, un segundo ANonce para uso en una segunda configuración de enlace con el punto de acceso posterior a la primera configuración de enlace.

[0140] Como otro ejemplo, la funcionalidad de AP puede implementarse utilizando instrucciones almacenadas en un medio legible por procesador. Por ejemplo, un medio particular puede almacenar instrucciones ejecutables para hacer que un procesador extraiga un mensaje de inicio de una solicitud de asociación sin protección recibida desde un dispositivo móvil. Las instrucciones también pueden ser ejecutables para hacer que el procesador extraiga una rMSK de un mensaje de respuesta recibido de un servidor de autentificación que responde al mensaje de inicio. Las instrucciones pueden ser además ejecutables para hacer que el procesador genere un ANonce y para generar una respuesta de asociación para ser enviada al dispositivo móvil, donde la respuesta de asociación incluye el ANonce. Otro medio particular puede almacenar instrucciones ejecutables por un procesador para enviar, desde un punto de acceso a un dispositivo móvil durante una primera configuración de enlace que usa un primer ANonce, un segundo ANonce para uso en una segunda configuración de enlace con el dispositivo móvil posterior a la primera configuración del enlace.

[0141] Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y pasos de algoritmo ilustrativos descritos en relación con los modos de realización divulgados en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito diversos componentes, bloques, módulos, circuitos y pasos ilustrativos, en general, en lo que respecta a su funcionalidad. Si tal funcionalidad se implementa como hardware, software o una combinación de los mismos, dependerá de la aplicación particular y de las selecciones de diseño impuestas sobre todo el sistema.

REIVINDICACIONES

1. Un procedimiento que puede hacerse funcionar en un punto de acceso (304), que comprende:

recibir (1802) una solicitud de asociación sin protección desde un dispositivo móvil (302), incluyendo la solicitud de asociación una estación creada para la ocasión, SNonce;

extraer (1804) un mensaje de inicio de la solicitud de asociación sin protección;

enviar (1806) el mensaje de inicio a un servidor de autentificación (308);

recibir un mensaje de respuesta desde el servidor de autentificación (308), en el que el mensaje de respuesta incluye una clave de sesión principal de re-autentificación, rMSK;

generar (1808) un punto de acceso creado para la ocasión, ANonce;

generar (1810) una clave transitoria de pares, PTK, usando la rMSK, el ANonce y el SNonce; y

enviar (1812) una respuesta de asociación al dispositivo móvil (302),
en el que la respuesta de asociación incluye el ANonce,
y la respuesta de asociación está protegida usando la PTK.

2. El procedimiento según la reivindicación 1, en el que la solicitud de asociación sin protección se envía basándose en un identificador de conjunto de servicios básicos, BSSID, del punto de acceso (304).

3. El procedimiento según la reivindicación 1, que comprende además enviar un protocolo de configuración principal dinámica, DHCP, mensaje de descubrimiento a un servidor DHCP.

4. El procedimiento según la reivindicación 3, que comprende además recibir un mensaje de confirmación de DHCP del servidor DHCP en respuesta al mensaje de descubrimiento de DHCP, en el que el mensaje de descubrimiento de DHCP indica una dirección de protocolo de internet, IP.

5. El procedimiento según la reivindicación 1, en el que la respuesta de asociación está protegida por integridad, y en la que se cifran elementos de información distintos del ANonce.

6. El procedimiento según la reivindicación 1, en el que el punto de acceso (304) se basa en el servidor de autentificación (308) que transmite un mensaje de respuesta con una rMSK obtenida como autentificación para el dispositivo móvil (302).

7. El procedimiento según la reivindicación 1, en el que la PTK se obtiene en el punto de acceso (304) antes de obtenerse en el dispositivo móvil (302).

8. Un programa informático que, cuando se ejecuta en un ordenador, comprende instrucciones para realizar un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 7.

9. Un aparato (304), que comprende:

medios para recibir una solicitud de asociación sin protección en un punto de acceso (304) desde un dispositivo móvil (302), incluyendo la solicitud de asociación una estación creada para la ocasión, SNonce;

medios para extraer un mensaje de inicio de la solicitud de asociación sin protección;

medios para enviar el mensaje de inicio a un servidor de autentificación (308);

medios para recibir un mensaje de respuesta desde el servidor de autentificación (308), en el que el mensaje de respuesta incluye una clave de sesión principal de re-autentificación, rMSK;

medios para generar un punto de acceso creado para la ocasión, ANonce;

medios para generar una clave transitoria de pares, PTK, usando la rMSK, el ANonce y el SNonce; y

medios para enviar una respuesta de asociación desde el punto de acceso (304) al dispositivo móvil (302), en el que la respuesta de asociación incluye el ANonce, y la respuesta de asociación está protegida usando la PTK.

10. El aparato (304) de la reivindicación 9, en el que la solicitud de asociación sin protección se envía basándose en un identificador de conjunto de servicios básicos, BSSID, del punto de acceso (304).

11. El aparato (304) de la reivindicación 9, que comprende además medios para enviar un protocolo de configuración principal dinámica, DHCP, mensaje de descubrimiento a un servidor DHCP.

12. El aparato (304) de la reivindicación 11, que comprende además medios para recibir un mensaje de confirmación de DHCP del servidor DHCP en respuesta al mensaje de descubrimiento de DHCP, en el que el mensaje de descubrimiento de DHCP indica una dirección de protocolo Internet, IP.

13. El aparato (304) de la reivindicación 9, en el que la respuesta de asociación está protegida por integridad, y en la que se cifran elementos de información distintos del ANonce.

14. El aparato (304) de la reivindicación 9, en el que el punto de acceso (304) se basa en el servidor de autentificación (308) que transmite un mensaje de respuesta con una rMSK obtenida como autentificación para el dispositivo móvil (302).

15. El aparato (304) de la reivindicación 9, en el que la PTK se obtiene en el punto de acceso (304) antes de obtenerse en el dispositivo móvil (302).

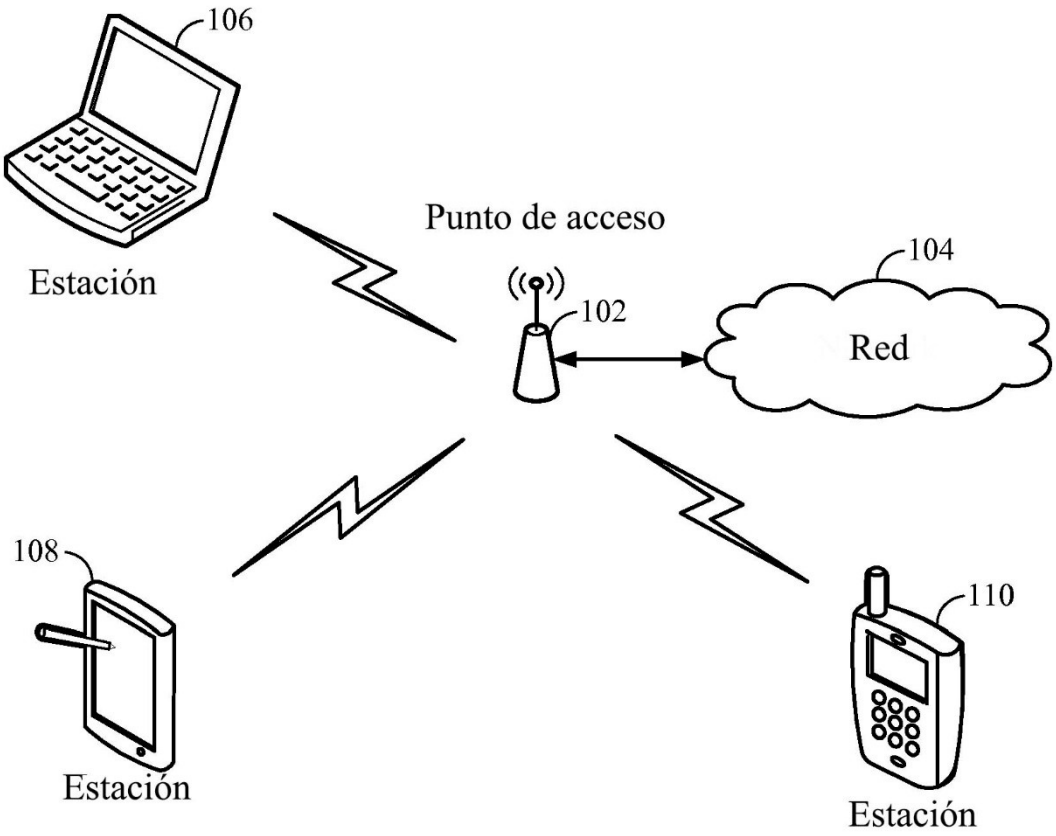
106
Estación
Punto de acceso
102
104
Red
108
Estación
110
Estación

FIG. 1

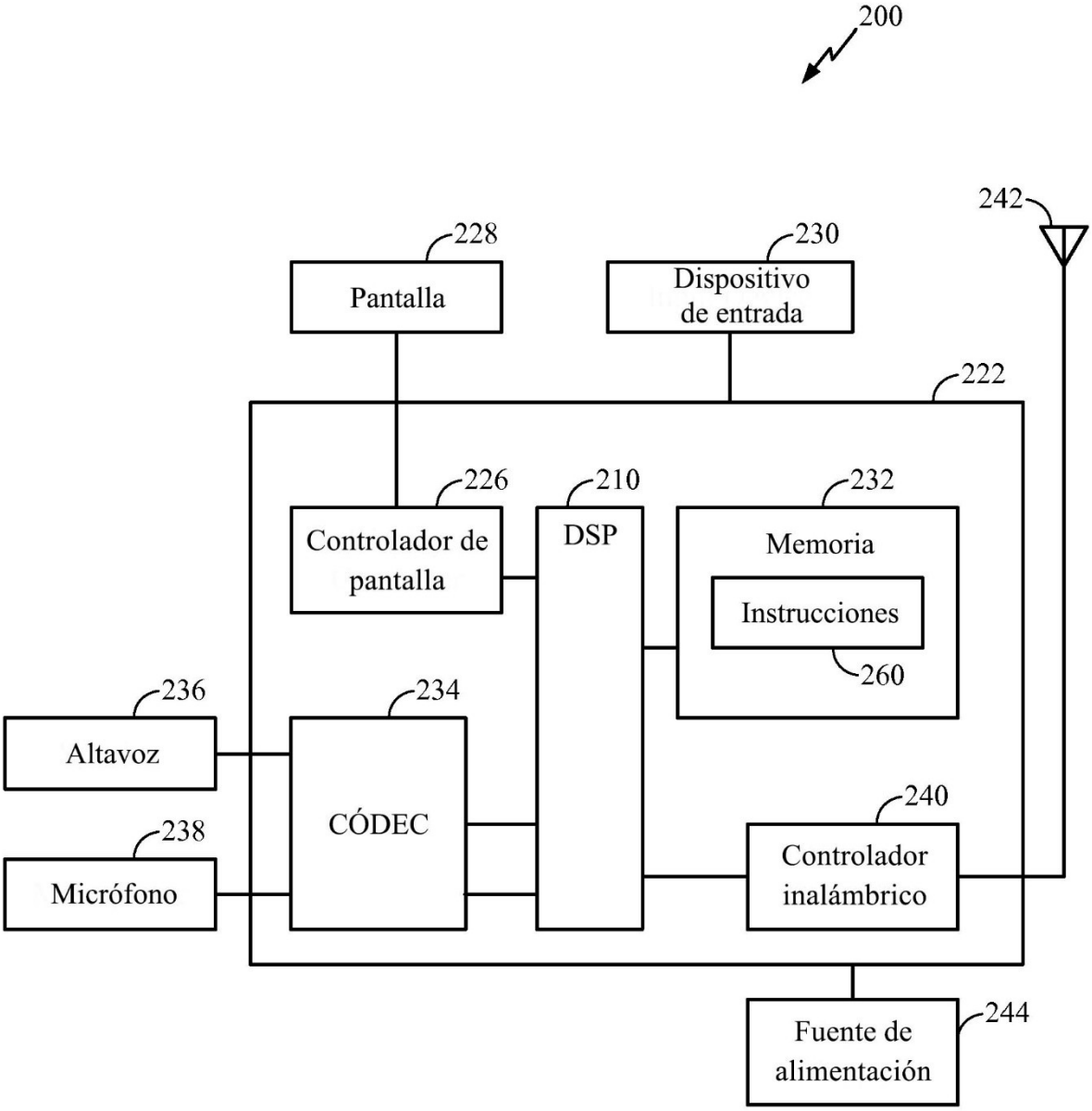
200
242
228
Pantalla
230
Dispositivo de entrada
222
226
Controlador de pantalla
210
DSP
232
Memoria
Instrucciones
260
236
Altavoz
234
CÓDEC
238
Micrófono
240
Controlador inalámbrico
244
Fuente de alimentación

FIG. 2

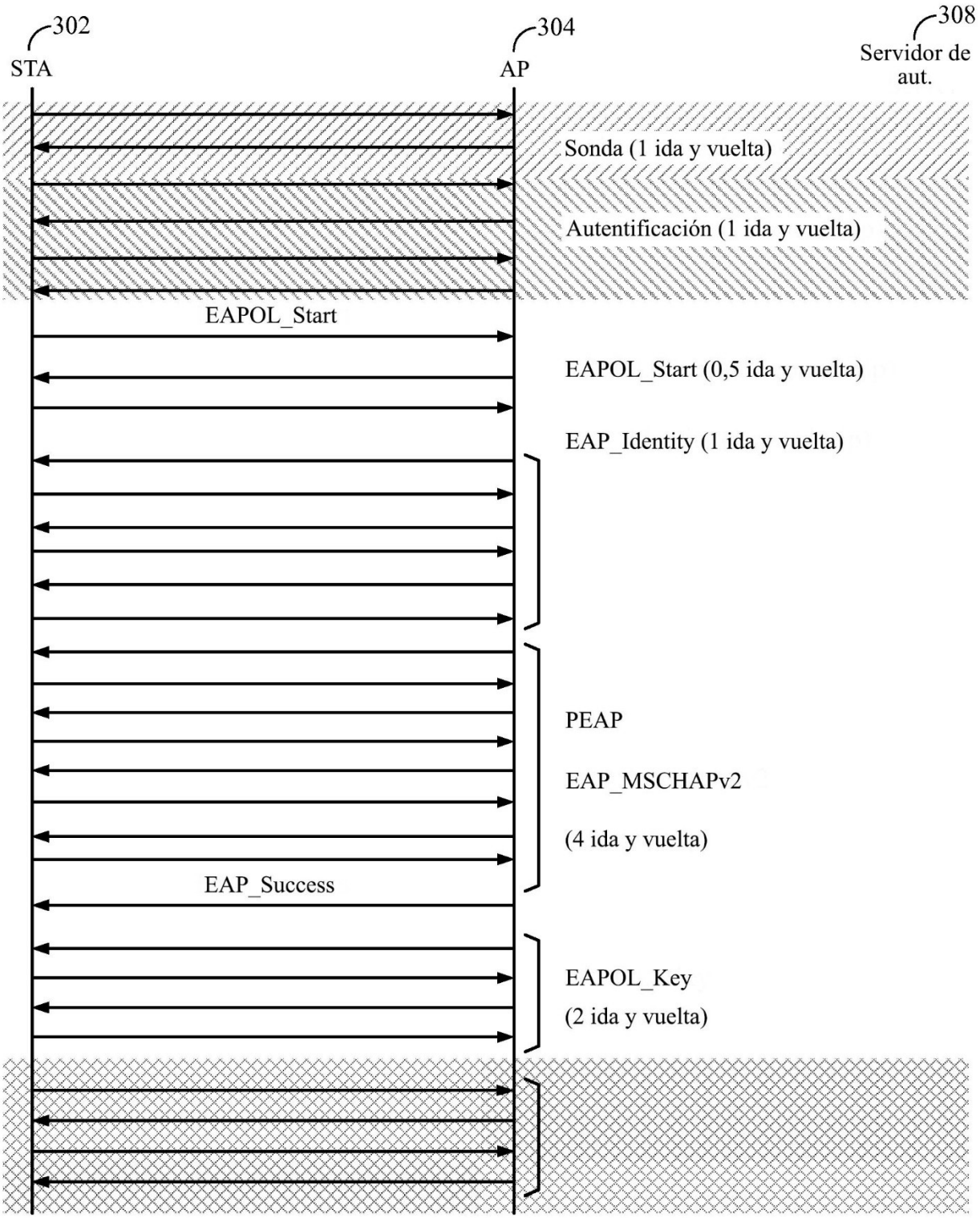
302
STA
304
AP
308
Servidor de aut.
Sonda (1 ida y vuelta)
Autentificación (1 ida y vuelta)
EAPOL_Start
EAPOL_Start (0,5 ida y vuelta)
EAP_Identity (1 ida y vuelta)
PEAP
EAP_MSCHAPv2
(4 ida y vuelta)
EAP_Success
EAPOL_Key
(2 ida y vuelta)

FIG. 3

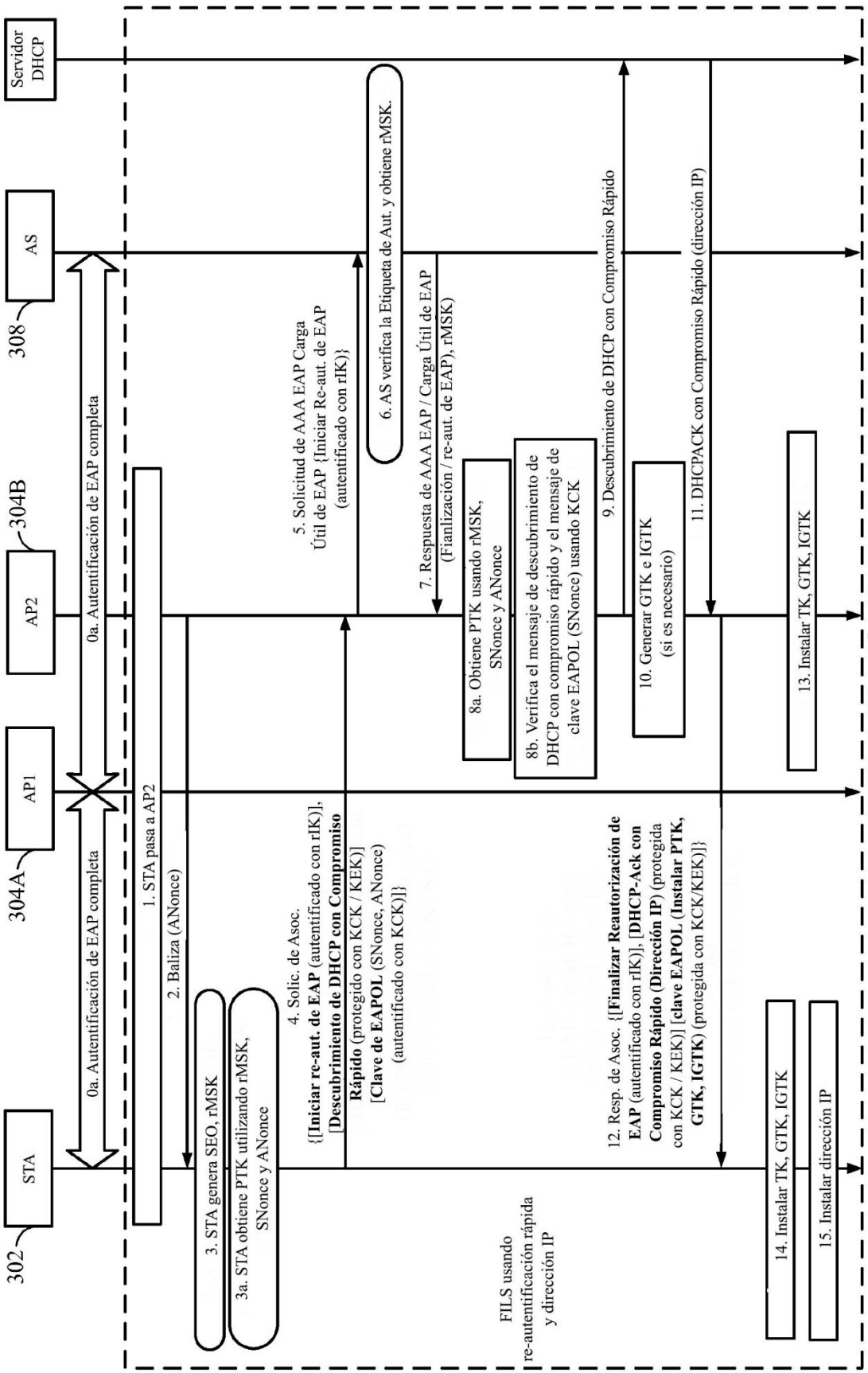

FIG. 4 (Opción 1)

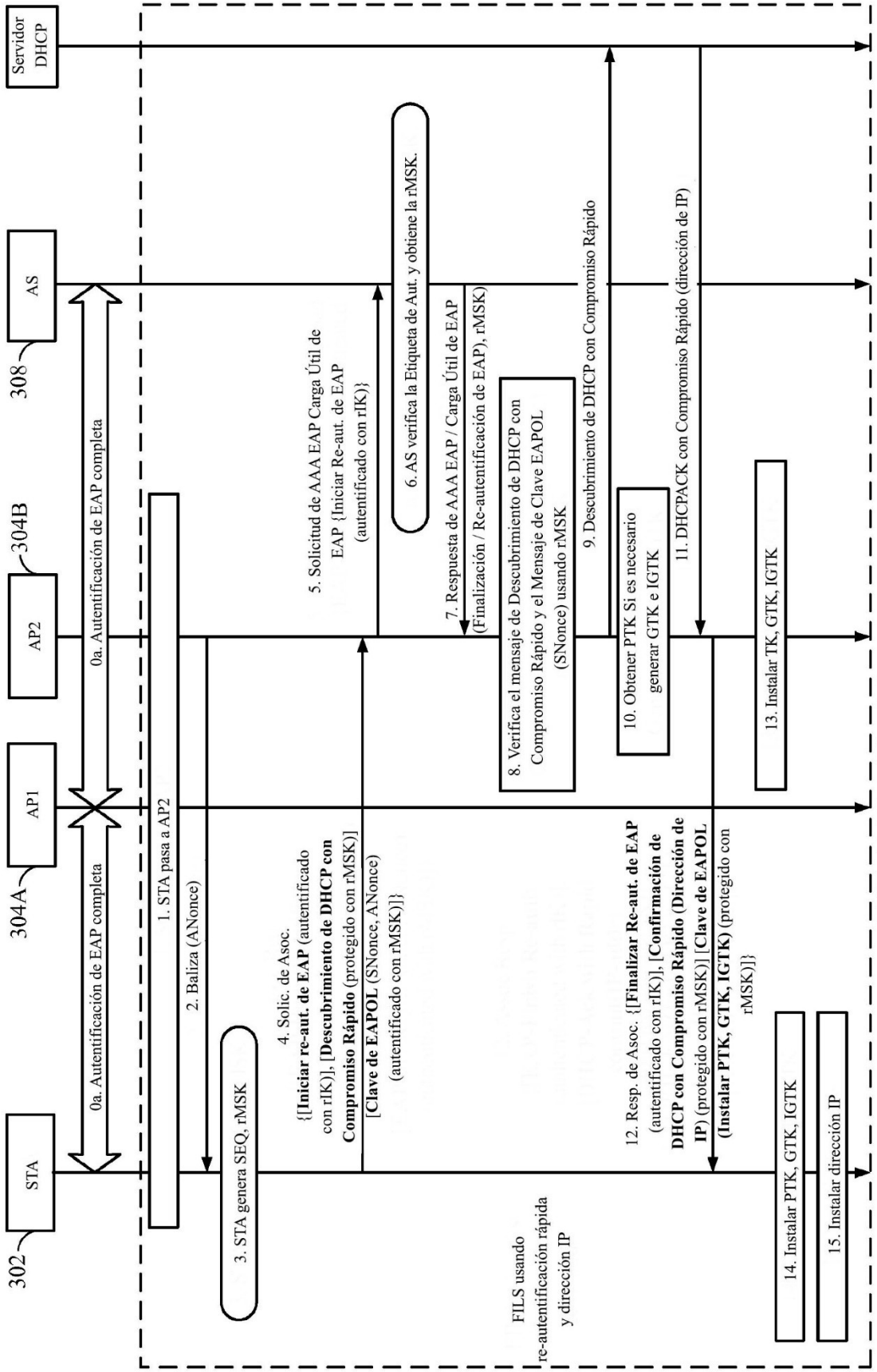

FIG. 5 (Opción 1a)

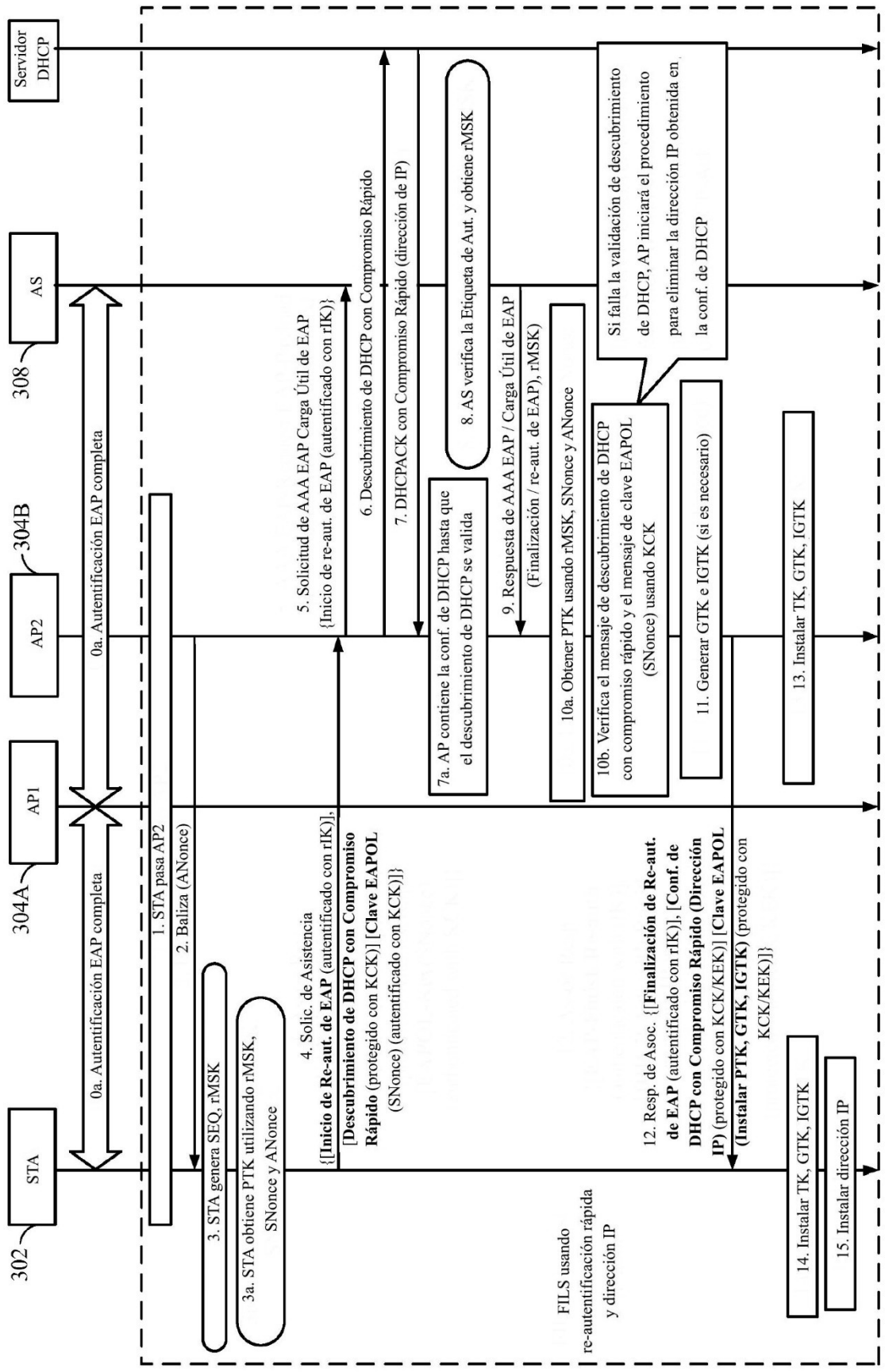

FIG. 6 (Opción 1b)

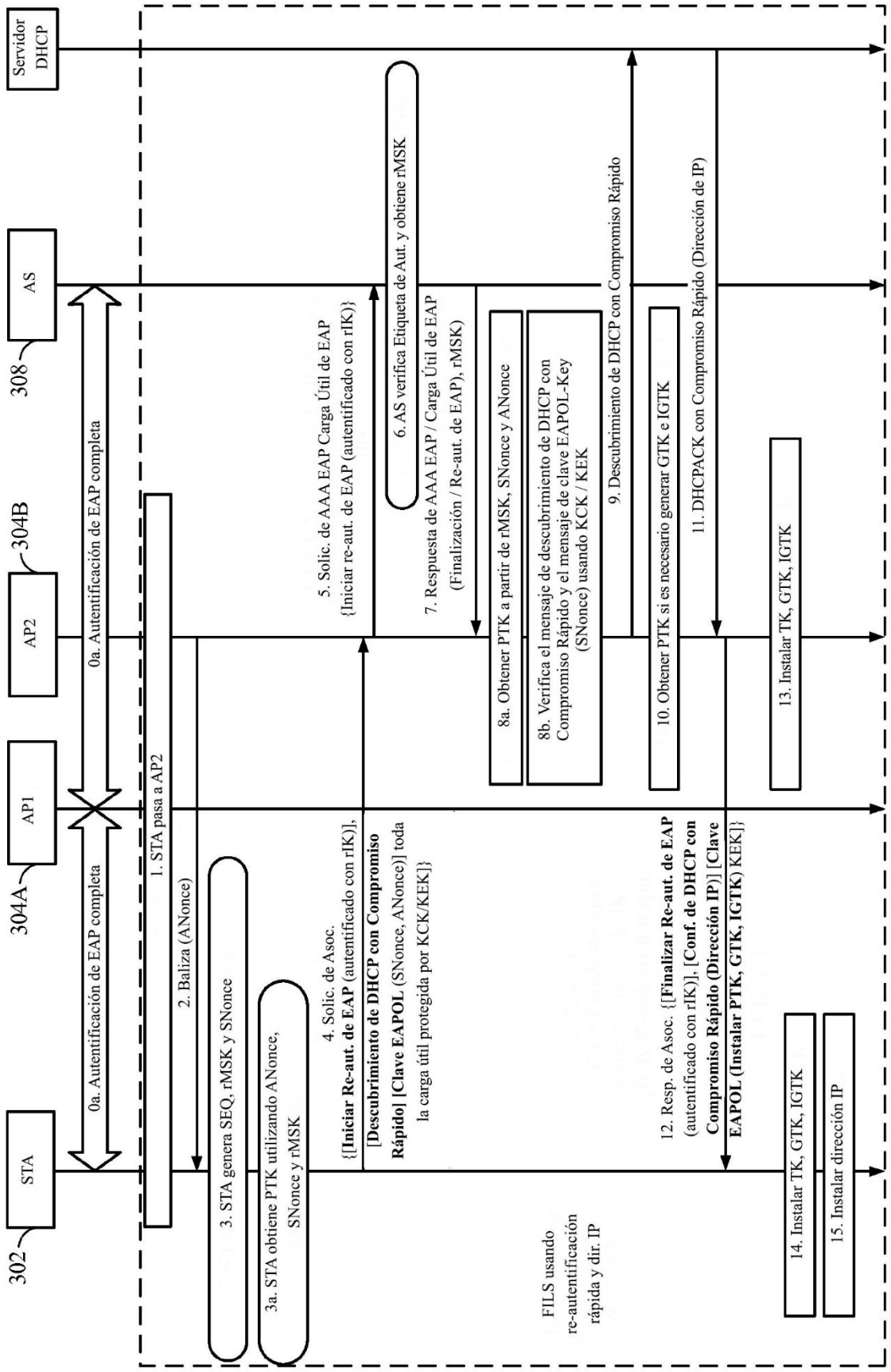

FIG. 7 (Opción 2)

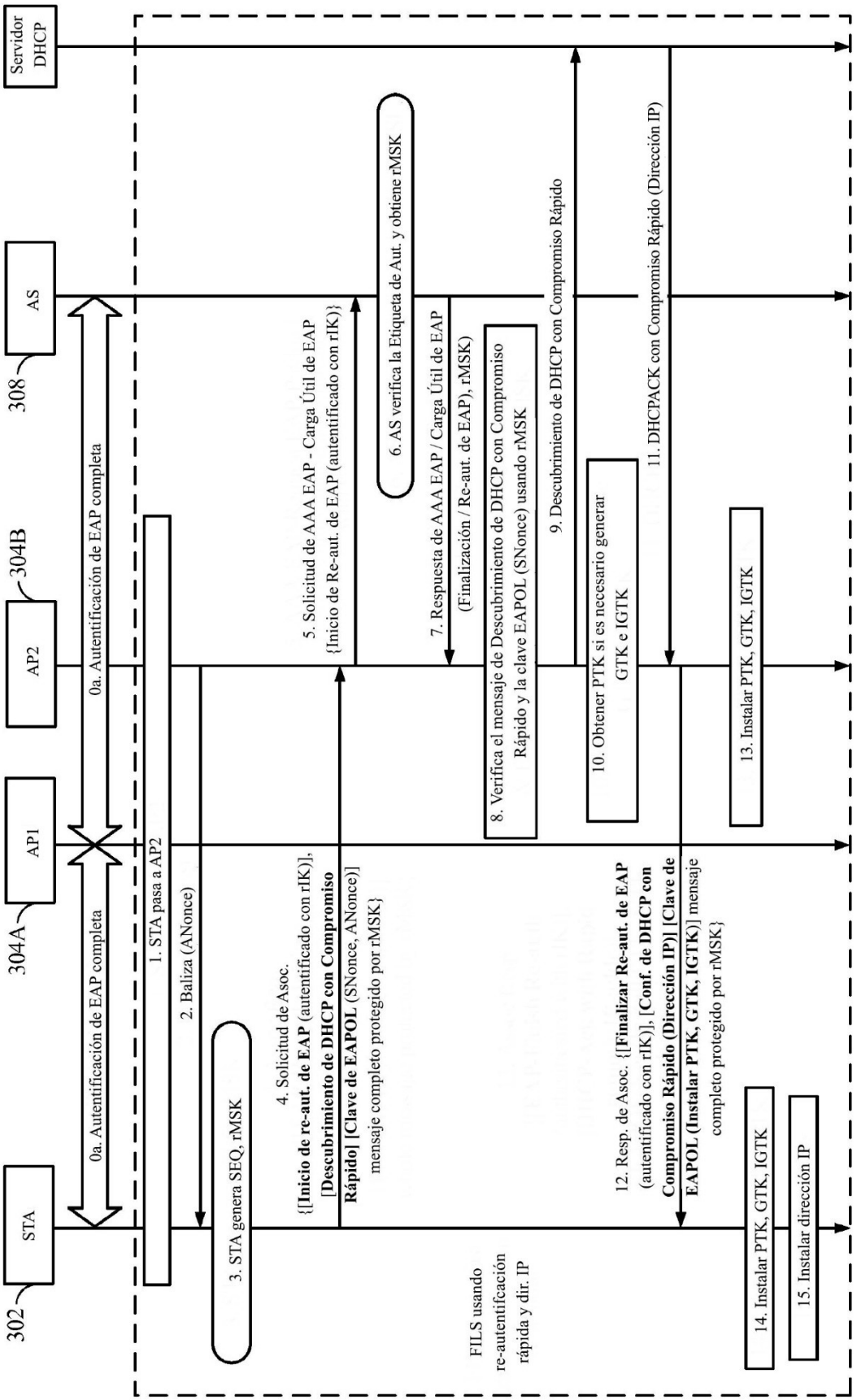

FIG. 8 (Opción 2a)

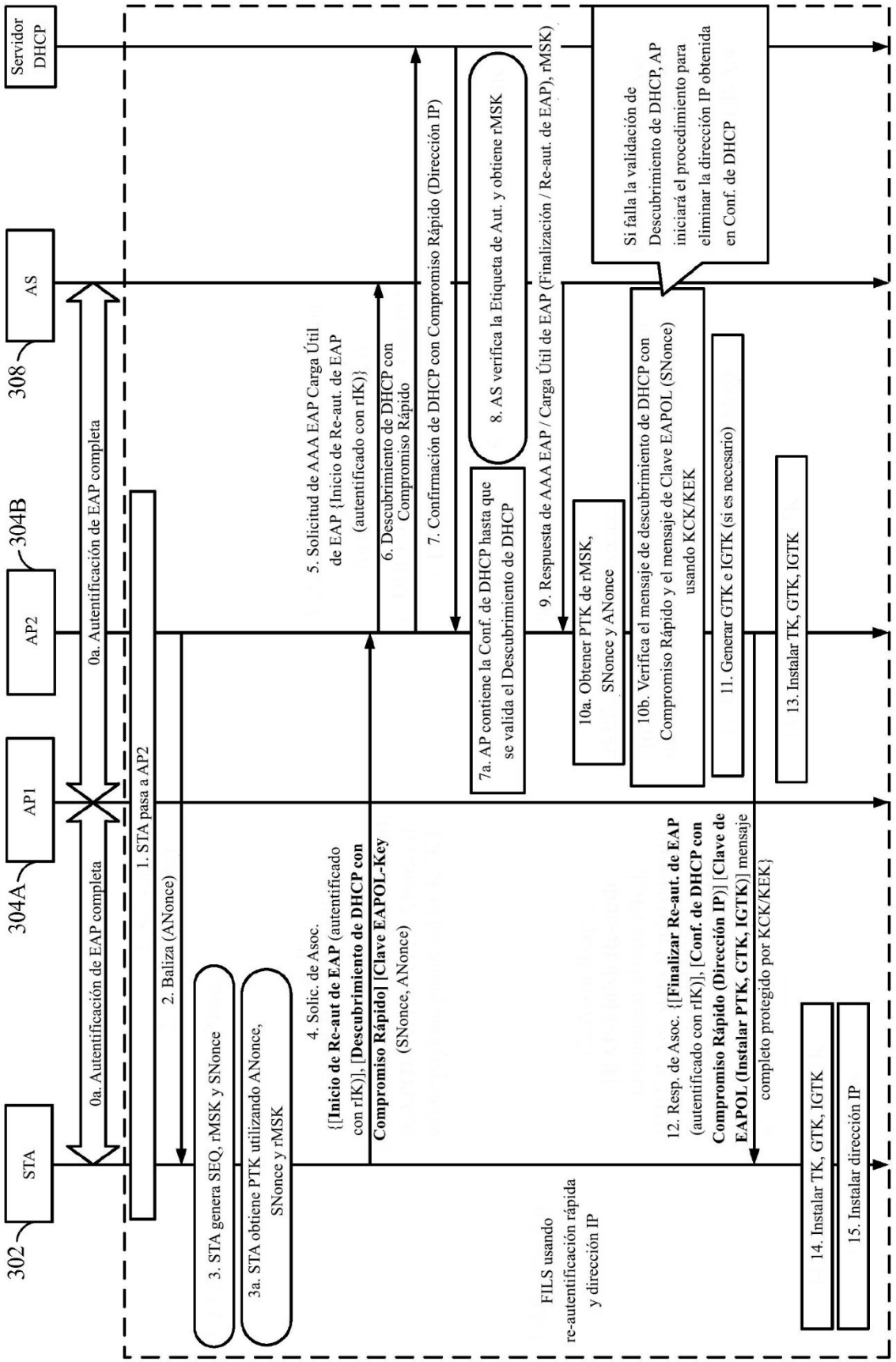

FIG. 9 (Opción 2b)

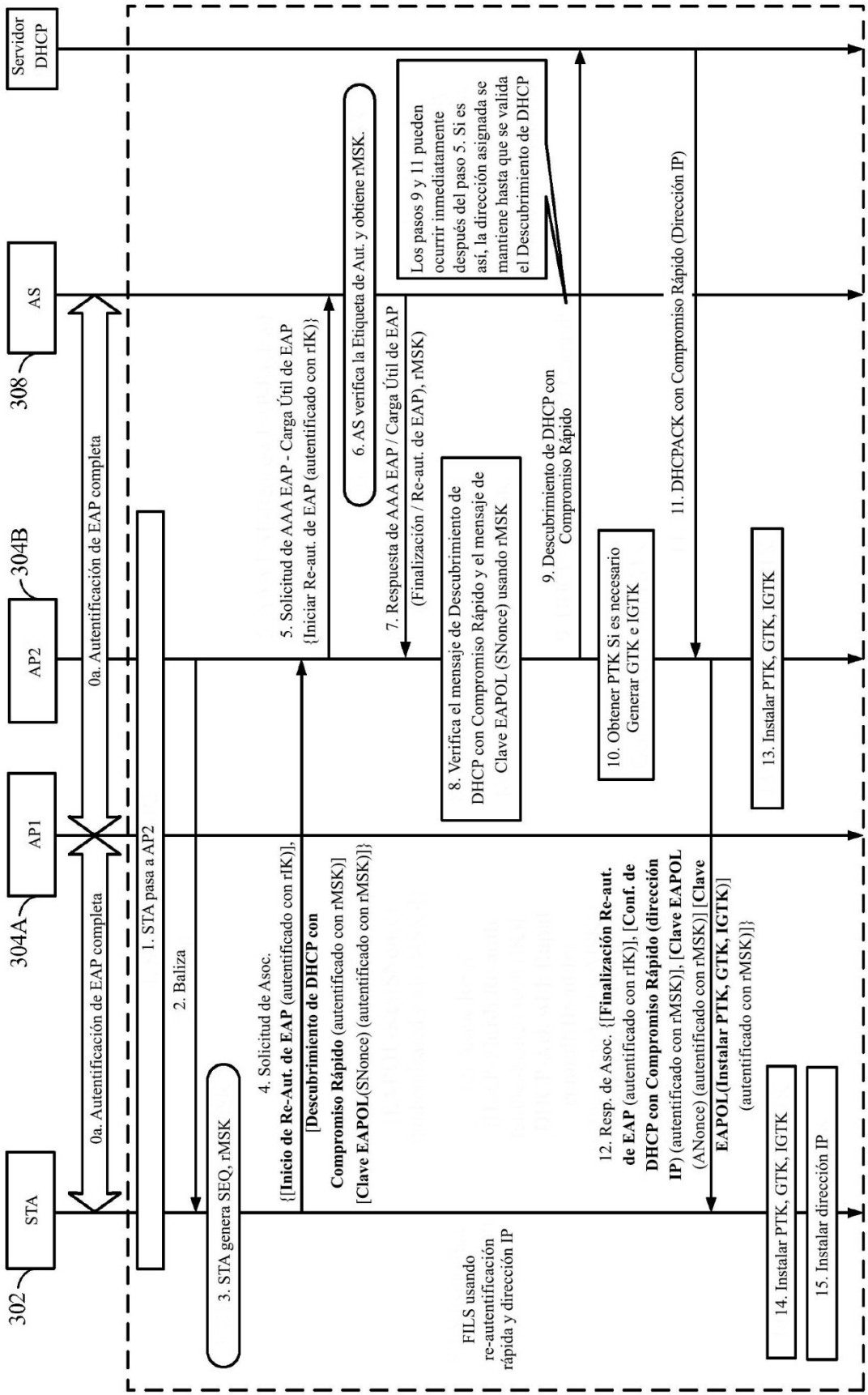

FIG. 10 (Opción 3)

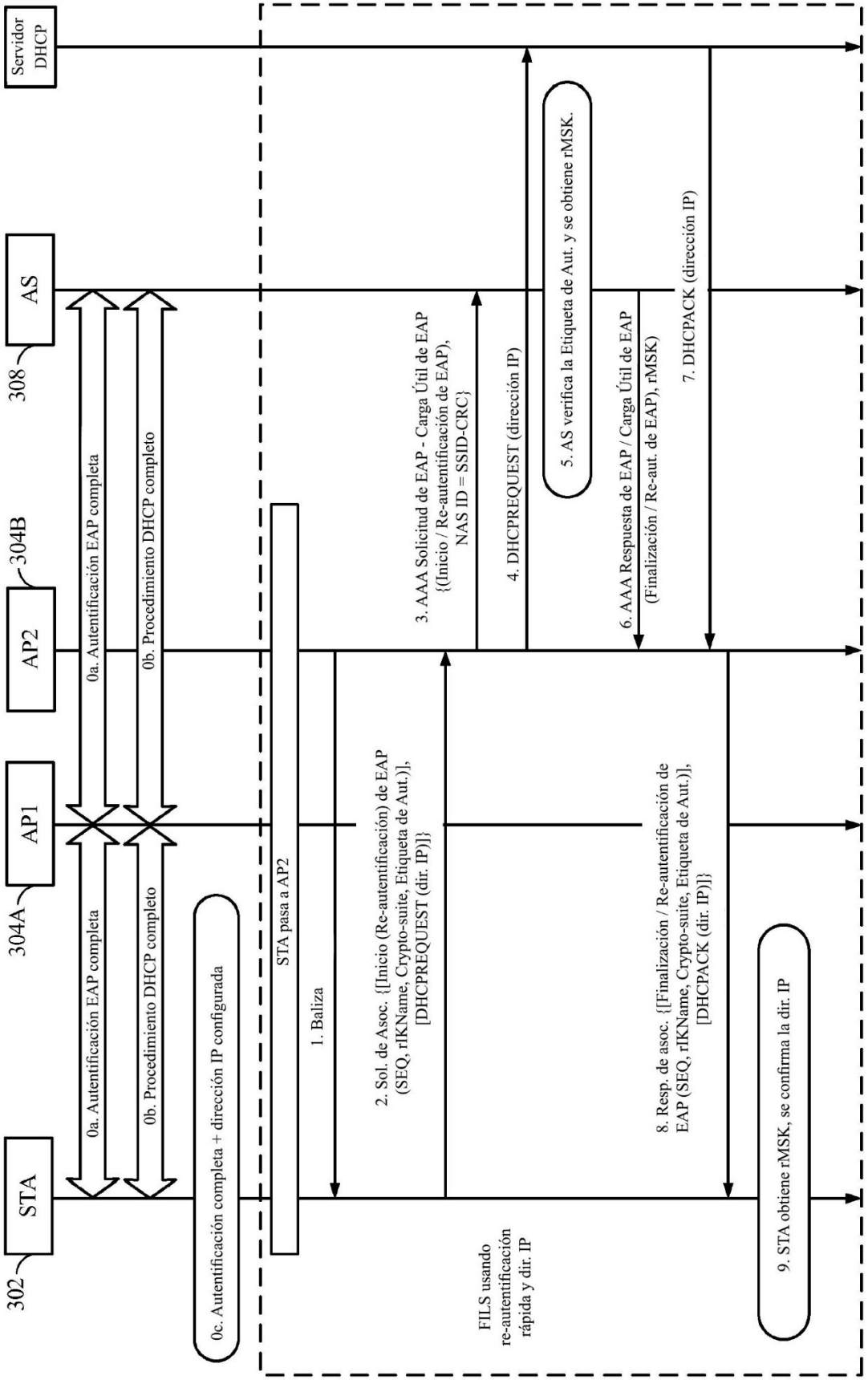

FIG. 11 (Opción 5)

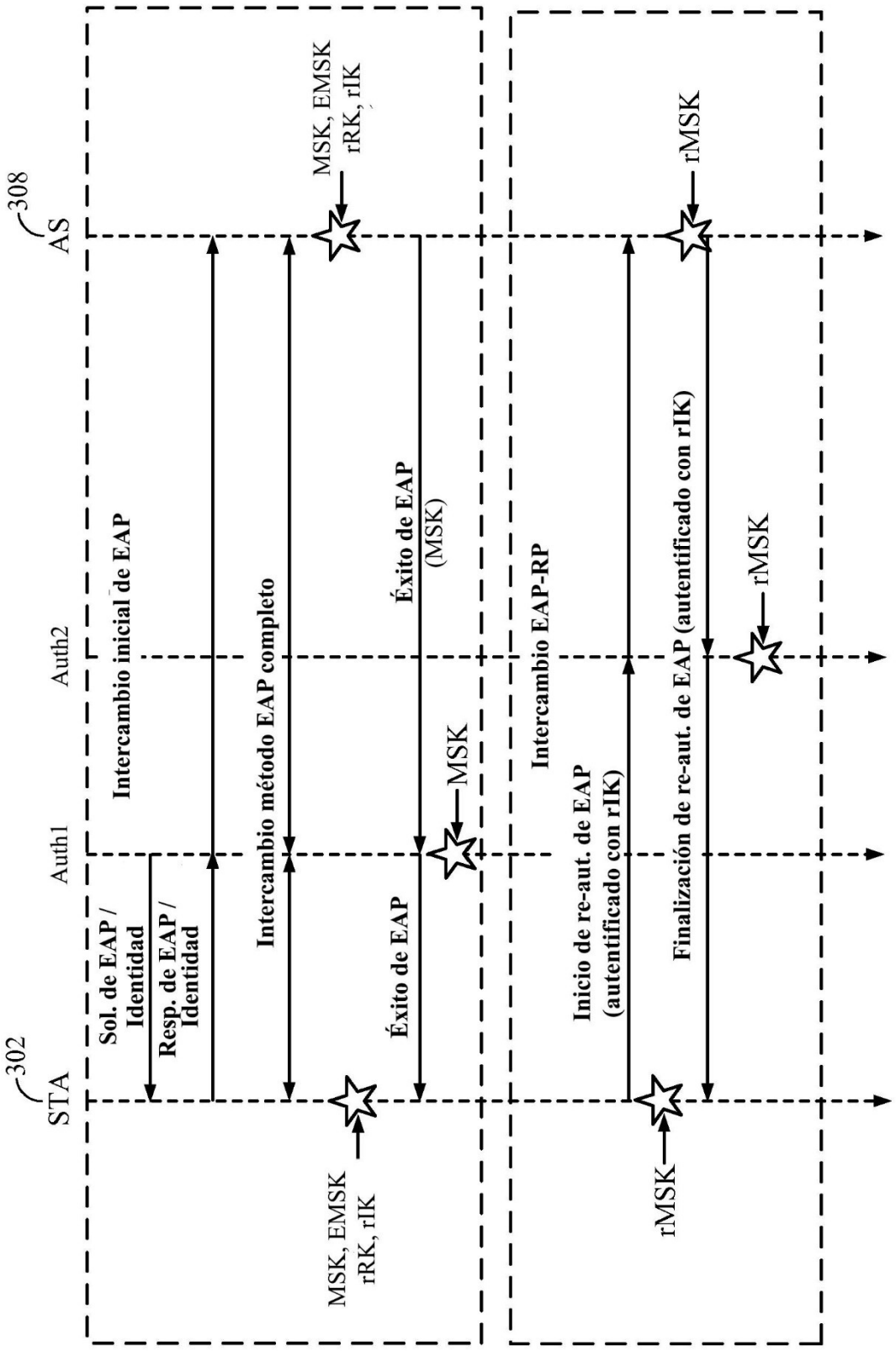
302
STA
Auth1
Auth2
308
AS
Sol. de EAP / Identidad
Resp. de EAP / Identidad
Intercambio inicial de EAP
Intercambio método EAP completo
Éxito de EAP
Éxito de EAP
(MSK)
MSK
MSK, EMSK
rRK, rIK
MSK, EMSK
rRK, rIK
Intercambio EAP-RP
Inicio de re-aut. de EAP
(autentificado con rIK)
Finalización de re-aut. de EAP (autentificado con rIK)
rMSK
rMSK
rMSK

FIG. 12

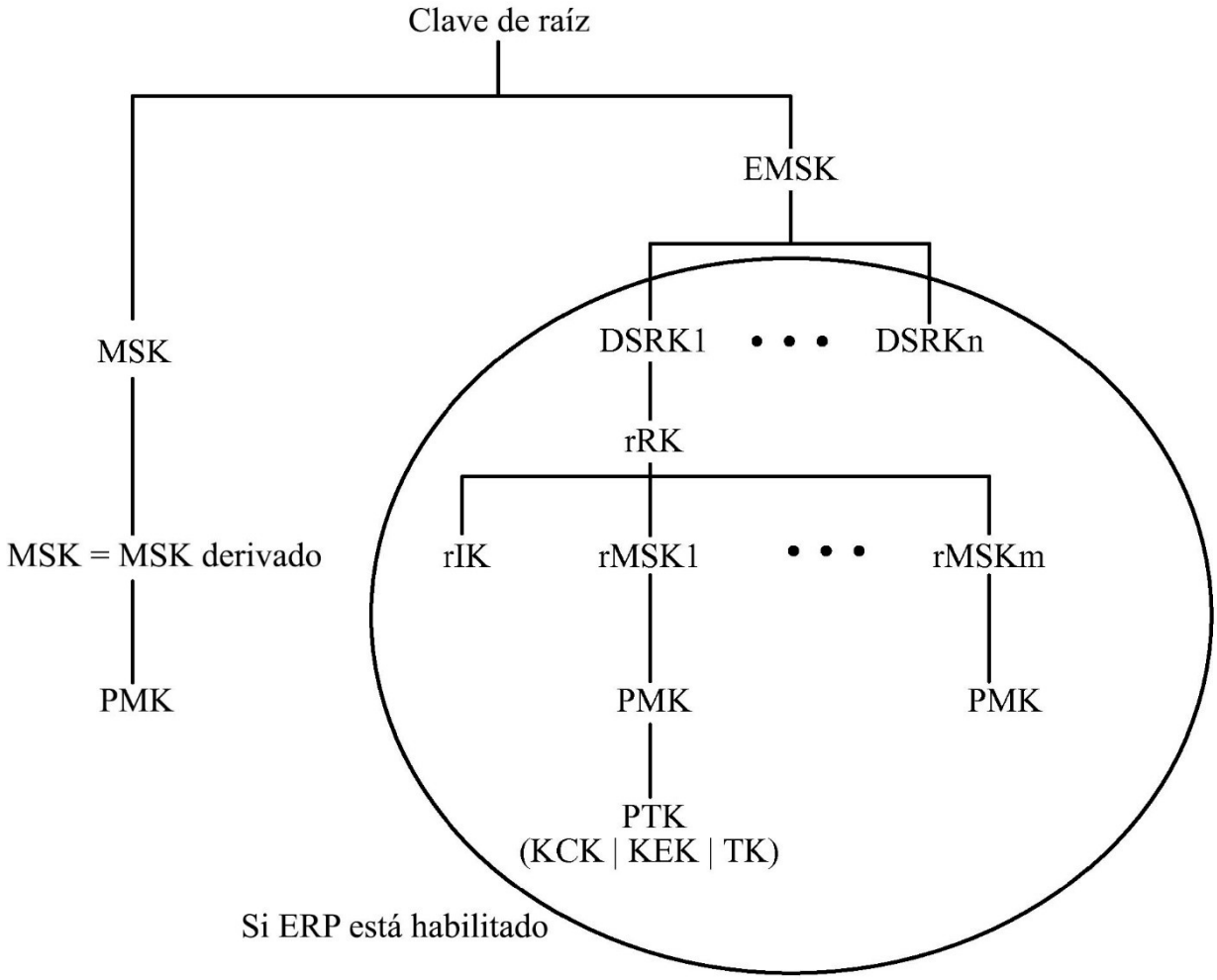
Clave de raíz
EMSK
MSK
DSRK1 • • • DSRKn
rRK
MSK = MSK derivado
rIK
rMSK1 • • • rMSKm
PMK
PMK
PMK
PTK
(KCK | KEK | TK)
Si ERP está habilitado

FIG. 13

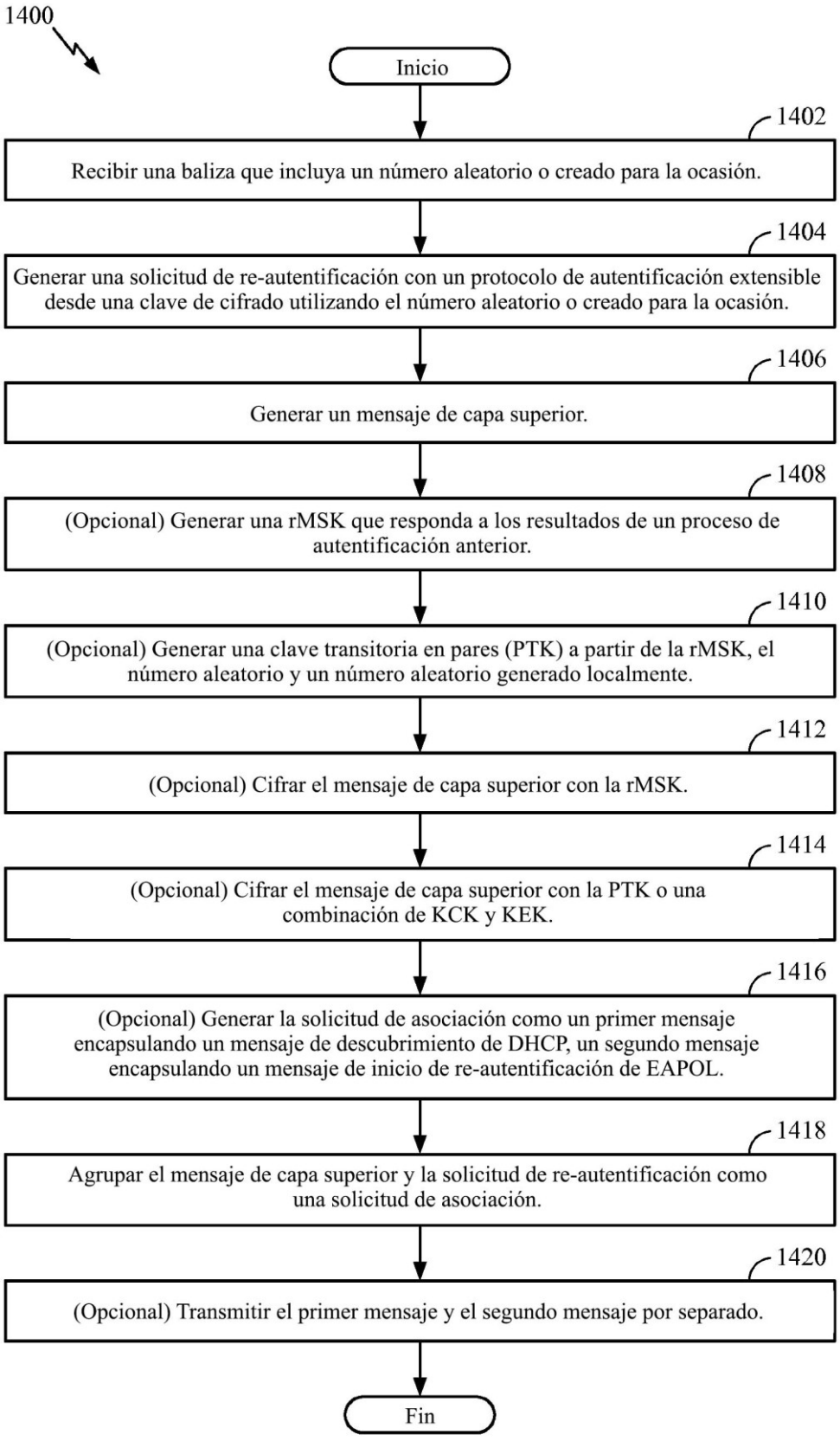
1400
Inicio
1402
Recibir una baliza que incluya un número aleatorio o creado para la ocasión.
1404
Generar una solicitud de re-autentificación con un protocolo de autentificación extensible desde una clave de cifrado utilizando el número aleatorio o creado para la ocasión.
1406
Generar un mensaje de capa superior.
1408
(Opcional) Generar una rMSK que responda a los resultados de un proceso de autentificación anterior.
1410
(Opcional) Generar una clave transitoria en pares (PTK) a partir de la rMSK, el número aleatorio y un número aleatorio generado localmente.
1412
(Opcional) Cifrar el mensaje de capa superior con la rMSK.
1414
(Opcional) Cifrar el mensaje de capa superior con la PTK o una combinación de KCK y KEK.
1416
(Opcional) Generar la solicitud de asociación como un primer mensaje encapsulando un mensaje de descubrimiento de DHCP, un segundo mensaje encapsulando un mensaje de inicio de re-autentificación de EAPOL.
1418
Agrupar el mensaje de capa superior y la solicitud de re-autentificación como una solicitud de asociación.
1420
(Opcional) Transmitir el primer mensaje y el segundo mensaje por separado.
Fin

FIG. 14

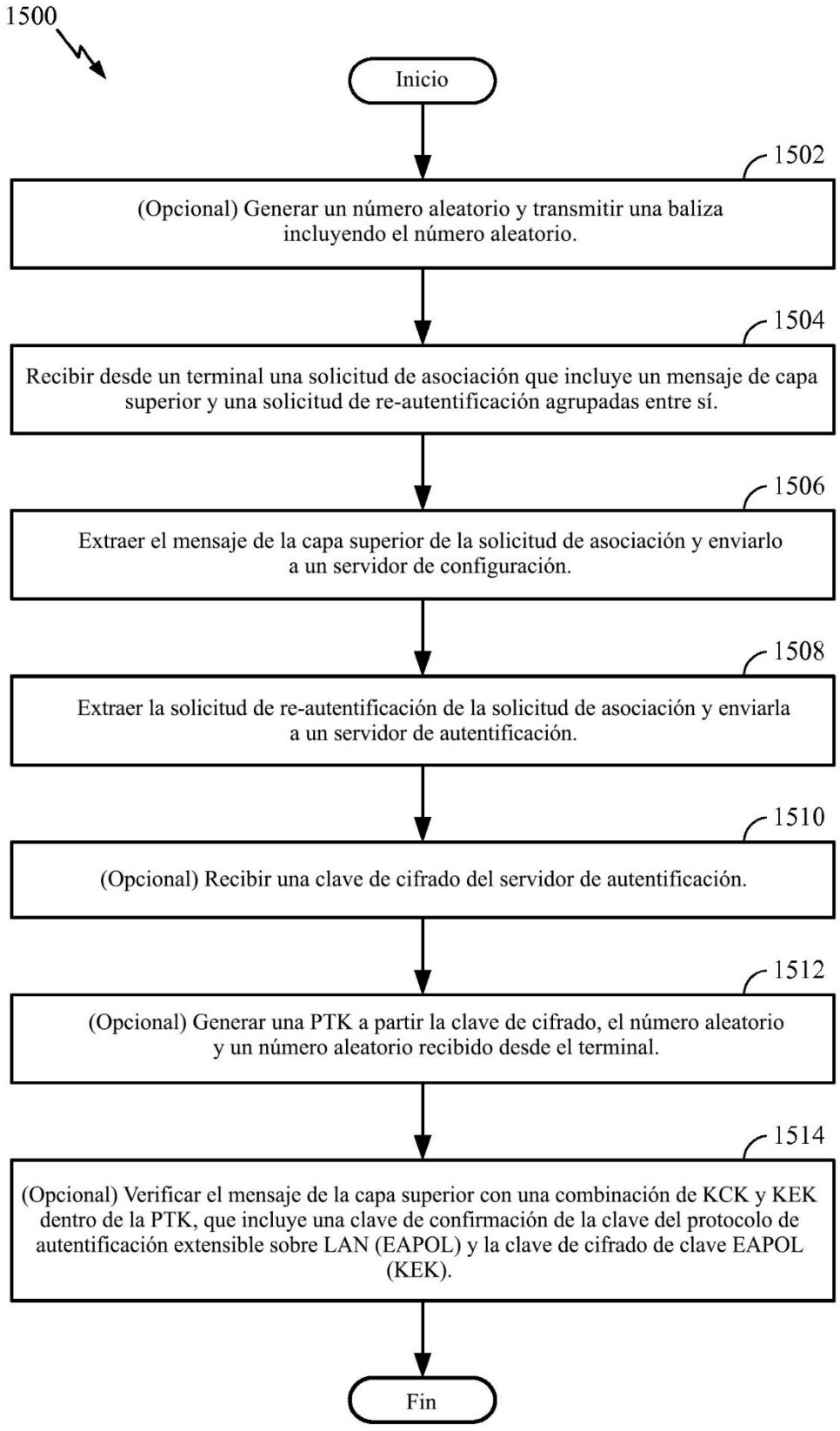
1500
Inicio
1502
(Opcional) Generar un número aleatorio y transmitir una baliza incluyendo el número aleatorio.
1504
Recibir desde un terminal una solicitud de asociación que incluye un mensaje de capa superior y una solicitud de re-autentificación agrupadas entre sí.
1506
Extraer el mensaje de la capa superior de la solicitud de asociación y enviarlo a un servidor de configuración.
1508
Extraer la solicitud de re-autentificación de la solicitud de asociación y enviarla a un servidor de autentificación.
1510
(Opcional) Recibir una clave de cifrado del servidor de autentificación.
1512
(Opcional) Generar una PTK a partir la clave de cifrado, el número aleatorio y un número aleatorio recibido desde el terminal.
1514
(Opcional) Verificar el mensaje de la capa superior con una combinación de KCK y KEK dentro de la PTK, que incluye una clave de confirmación de la clave del protocolo de autentificación extensible sobre LAN (EAPOL) y la clave de cifrado de clave EAPOL (KEK).
Fin

FIG. 15

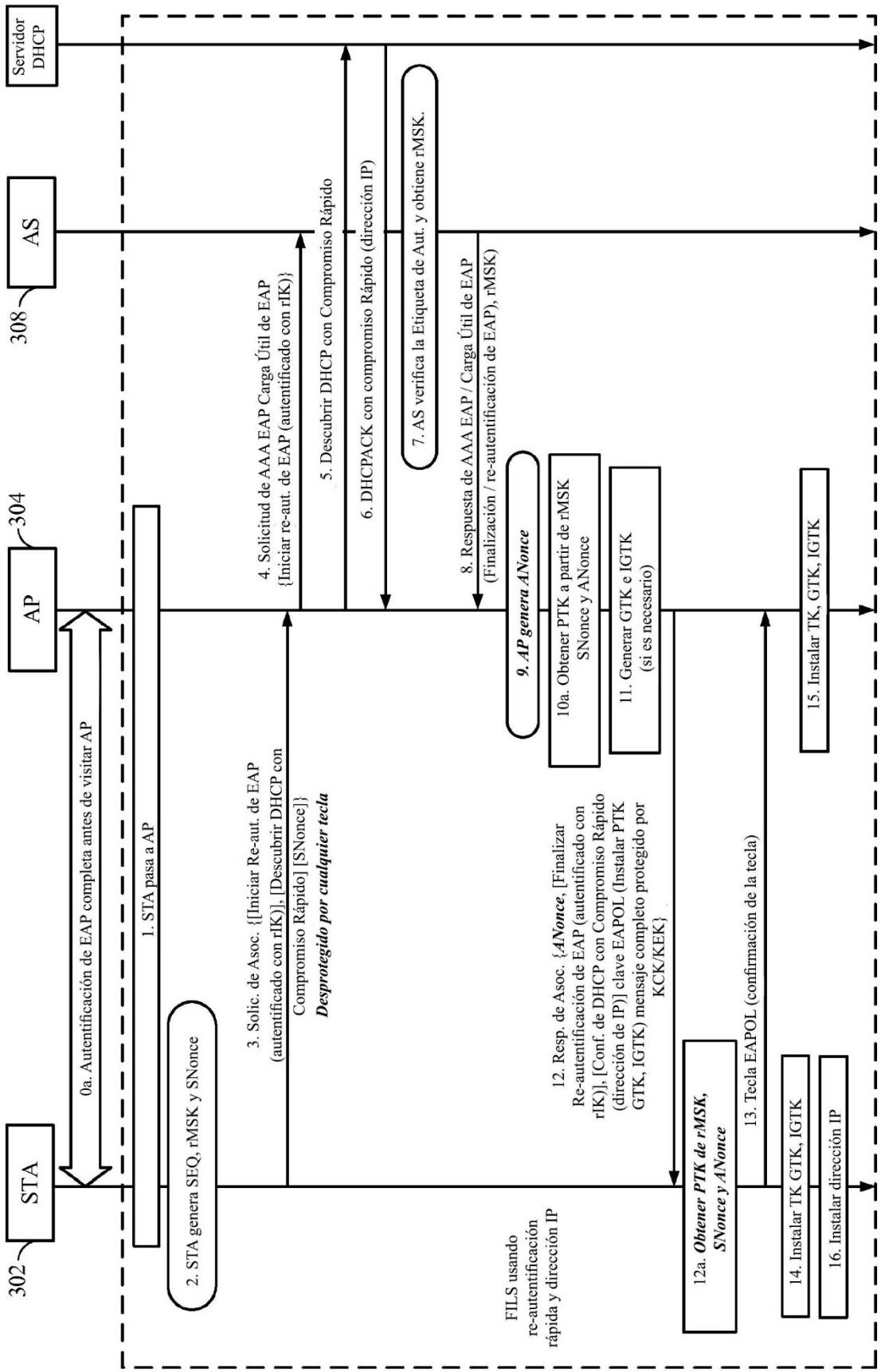
Servidor DHCP
AS
308
AP
304
STA
302
0a. Autentificación de EAP completa antes de visitar AP
1. STA pasa a AP
2. STA genera SEQ, rMSK y SNonce
3. Solic. de Asoc. {[Iniciar Re-aut. de EAP (autentificado con rIK)], [Descubrir DHCP con Compromiso Rápido] [SNonce]}
Desprotegido por cualquier tecla
4. Solicitud de AAA EAP Carga Útil de EAP {Iniciar re-aut. de EAP (autentificado con rIK)}
5. Descubrir DHCP con Compromiso Rápido
6. DHCPACK con compromiso Rápido (dirección IP)
7. AS verifica la Etiqueta de Aut. y obtiene rMSK.
8. Respuesta de AAA EAP / Carga Útil de EAP (Finalización / re-autentificación de EAP), rMSK)
9. AP genera ANonce
10a. Obtener PTK a partir de rMSK SNonce y ANonce
11. Generar GTK e IGTK (si es necesario)
12. Resp. de Asoc. {ANonce, [Finalizar Re-autentificación de EAP (autentificado con rIK)], [Conf. de DHCP con Compromiso Rápido (dirección de IP)] clave EAPOL (Instalar PTK GTK, IGTK) mensaje completo protegido por KCK/KEK}
12a. Obtener PTK de rMSK, SNonce y ANonce
13. Tecla EAPOL (confirmación de la tecla)
14. Instalar TK GTK, IGTK
15. Instalar TK, GTK, IGTK
16. Instalar dirección IP
FILS usando re-autentificación rápida y dirección IP

FIG. 16

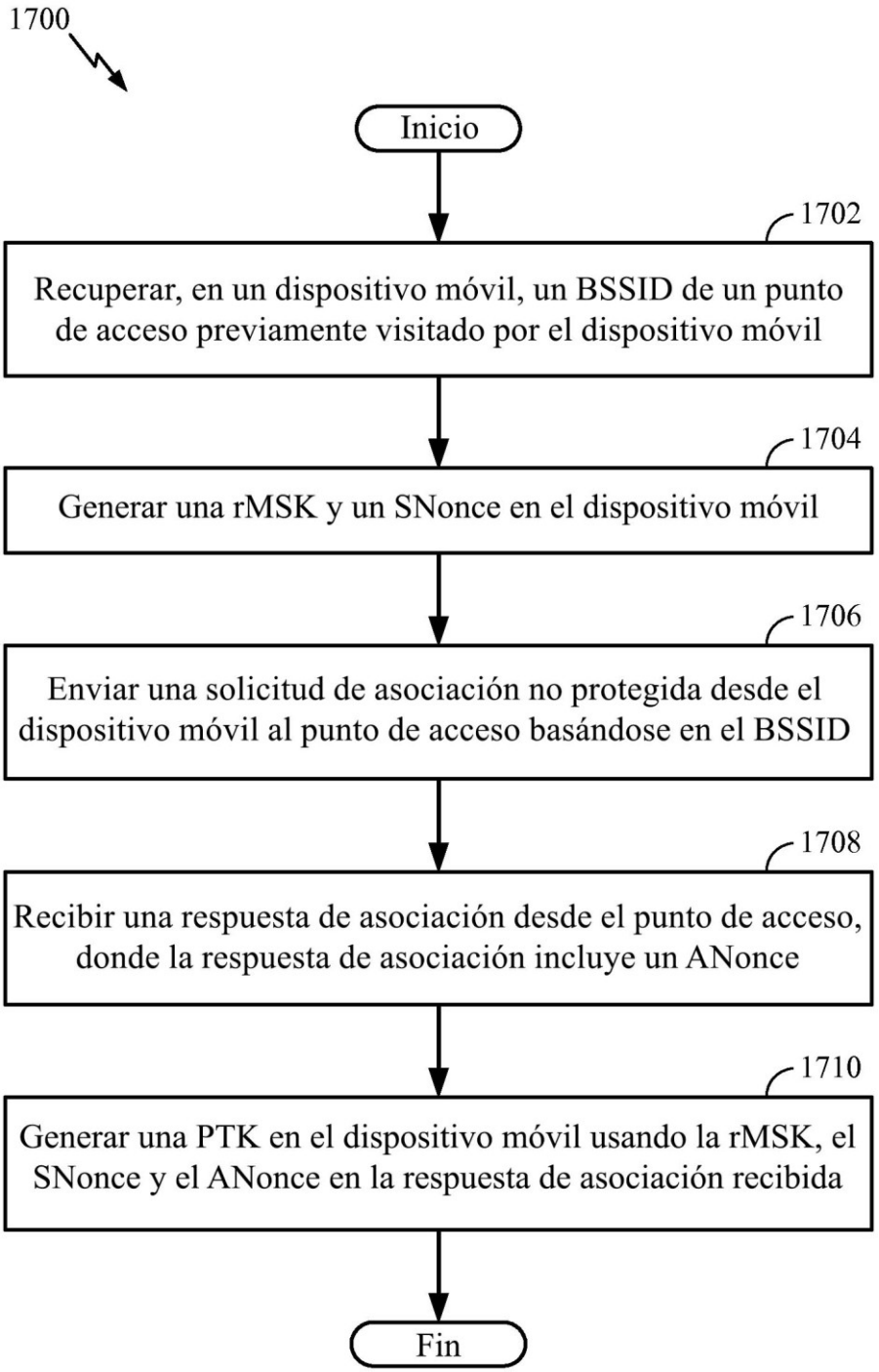
1700
Inicio
1702
Recuperar, en un dispositivo móvil, un BSSID de un punto de acceso previamente visitado por el dispositivo móvil
1704
Generar una rMSK y un SNonce en el dispositivo móvil
1706
Enviar una solicitud de asociación no protegida desde el dispositivo móvil al punto de acceso basándose en el BSSID
1708
Recibir una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un ANonce
1710
Generar una PTK en el dispositivo móvil usando la rMSK, el SNonce y el ANonce en la respuesta de asociación recibida
Fin

FIG. 17

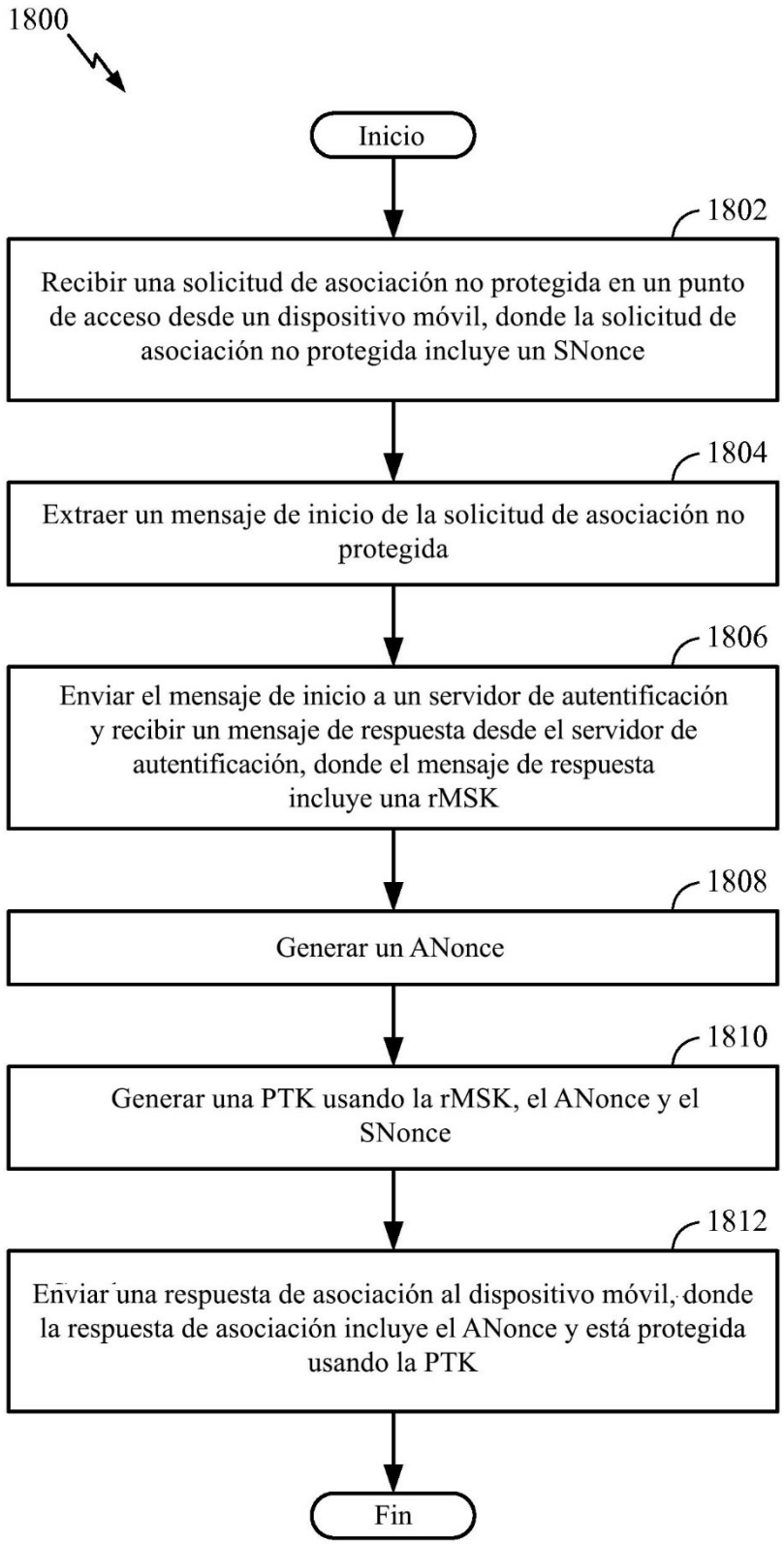
1800
Inicio
1802
Recibir una solicitud de asociación no protegida en un punto de acceso desde un dispositivo móvil, donde la solicitud de asociación no protegida incluye un SNonce
1804
Extraer un mensaje de inicio de la solicitud de asociación no protegida
1806
Enviar el mensaje de inicio a un servidor de autentificación y recibir un mensaje de respuesta desde el servidor de autentificación, donde el mensaje de respuesta incluye una rMSK
1808
Generar un ANonce
1810
Generar una PTK usando la rMSK, el ANonce y el SNonce
1812
Enviar una respuesta de asociación al dispositivo móvil, donde la respuesta de asociación incluye el ANonce y está protegida usando la PTK
Fin

FIG. 18

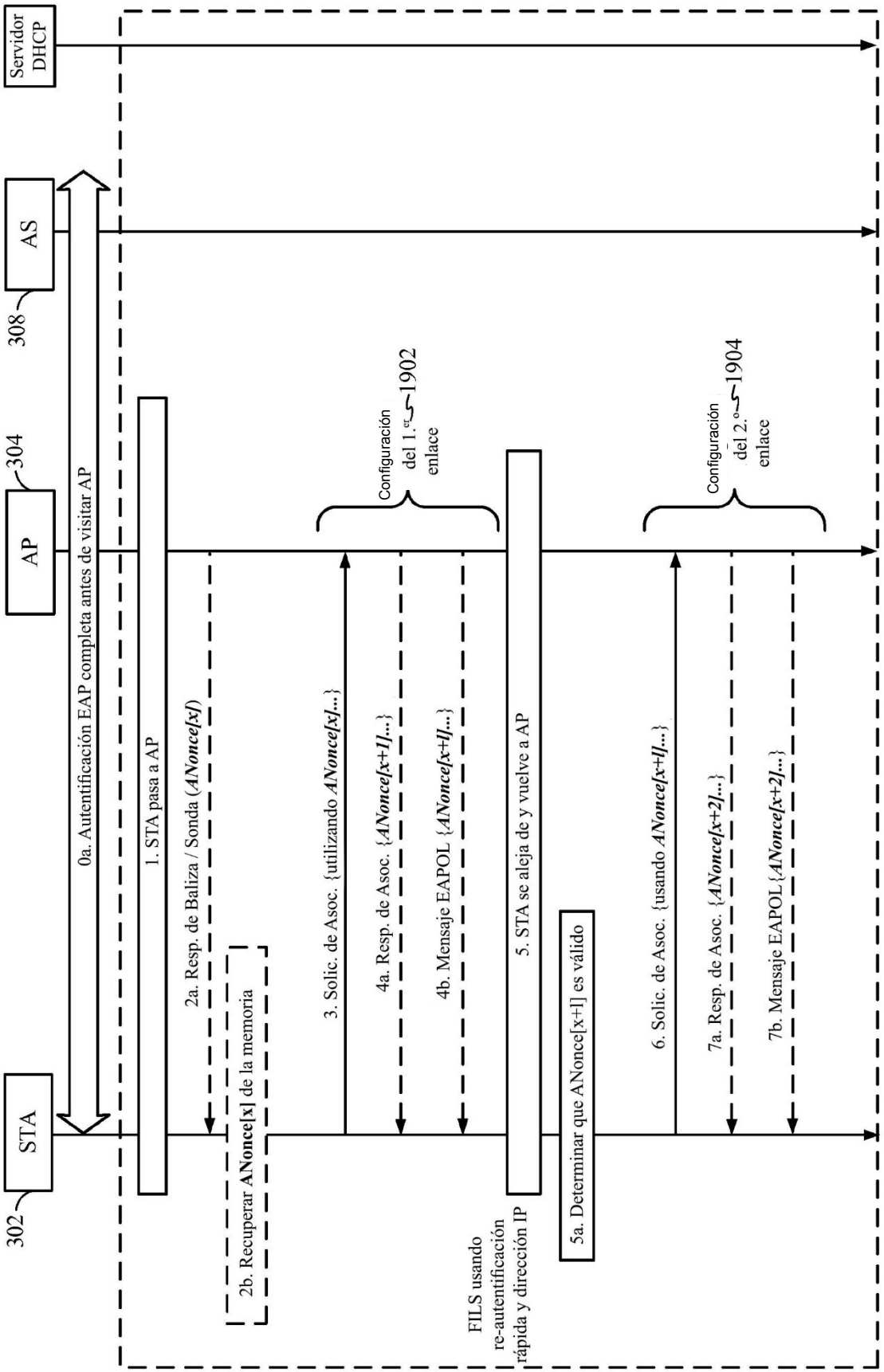
Servidor DHCP
AS
308
AP
304
STA
302
0a. Autentificación EAP completa antes de visitar AP
1. STA pasa a AP
2a. Resp. de Baliza / Sonda (ANonce[x])
2b. Recuperar ANonce[x] de la memoria
3. Solic. de Asoc. {utilizando ANonce[x]...}
4a. Resp. de Asoc. {ANonce[x+1]...}
4b. Mensaje EAPOL {ANonce[x+1]...}
Configuración del 1.er enlace
1902
FILS usando re-autentificación rápida y dirección IP
5. STA se aleja de y vuelve a AP
5a. Determinar que ANonce[x+1] es válido
6. Solic. de Asoc. {usando ANonce[x+1]...}
7a. Resp. de Asoc. {ANonce[x+2]...}
7b. Mensaje EAPOL{ANonce[x+2]...}
Configuración del 2.º enlace
1904

FIG. 19

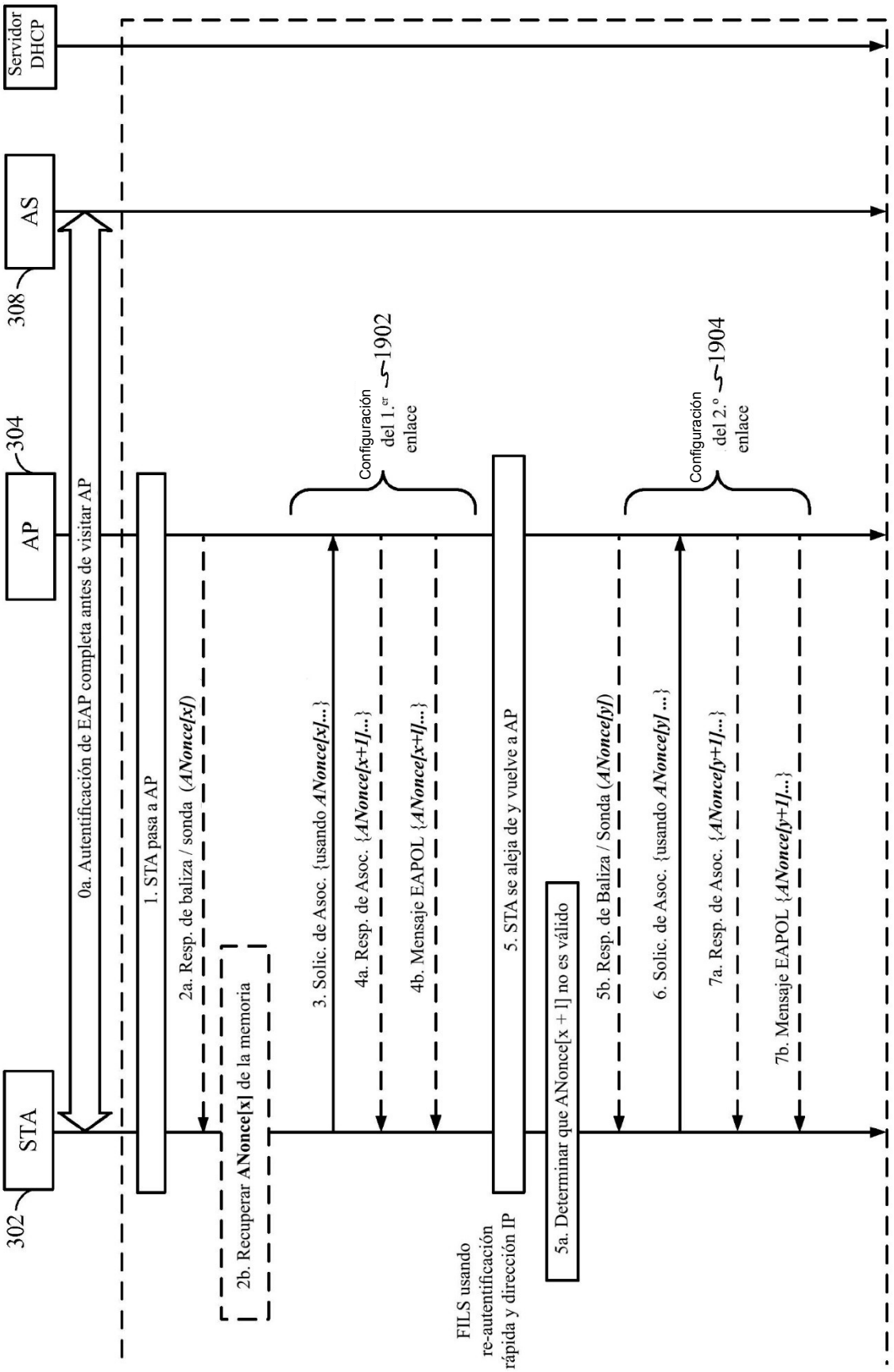
Servidor DHCP
AS
308
AP
304
STA
302
0a. Autentificación de EAP completa antes de visitar AP
1. STA pasa a AP
2a. Resp. de baliza / sonda (ANonce[x])
2b. Recuperar ANonce[x] de la memoria
3. Solic. de Asoc. {usando ANonce[x]...}
4a. Resp. de Asoc. {ANonce[x+1]...}
4b. Mensaje EAPOL {ANonce[x+1]...}
Configuración del 1.er enlace
1902
5. STA se aleja de y vuelve a AP
FILS usando re-autentificación rápida y dirección IP
5a. Determinar que ANonce[x + 1] no es válido
5b. Resp. de Baliza / Sonda (ANonce[y])
6. Solic. de Asoc. {usando ANonce[y] ...}
7a. Resp. de Asoc. {ANonce[y+1]...}
7b. Mensaje EAPOL {ANonce[y+1]...}
Configuración del 2.º enlace
1904

FIG. 20

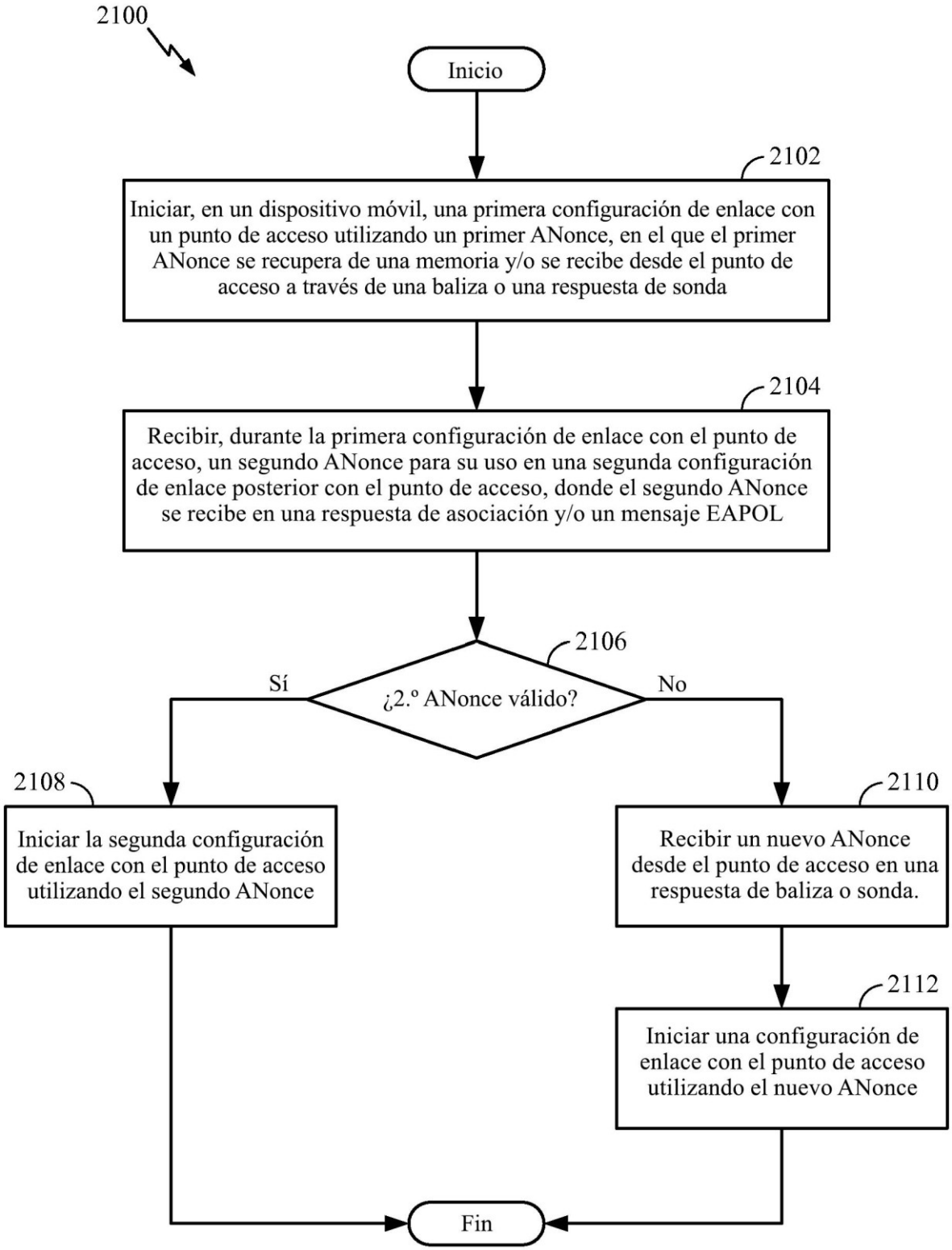
2100
Inicio
2102
Iniciar, en un dispositivo móvil, una primera configuración de enlace con un punto de acceso utilizando un primer ANonce, en el que el primer ANonce se recupera de una memoria y/o se recibe desde el punto de acceso a través de una baliza o una respuesta de sonda
2104
Recibir, durante la primera configuración de enlace con el punto de acceso, un segundo ANonce para su uso en una segunda configuración de enlace posterior con el punto de acceso, donde el segundo ANonce se recibe en una respuesta de asociación y/o un mensaje EAPOL
2106
¿2.º ANonce válido?
Sí
No
2108
Iniciar la segunda configuración de enlace con el punto de acceso utilizando el segundo ANonce
2110
Recibir un nuevo ANonce desde el punto de acceso en una respuesta de baliza o sonda.
2112
Iniciar una configuración de enlace con el punto de acceso utilizando el nuevo ANonce
Fin

FIG. 21

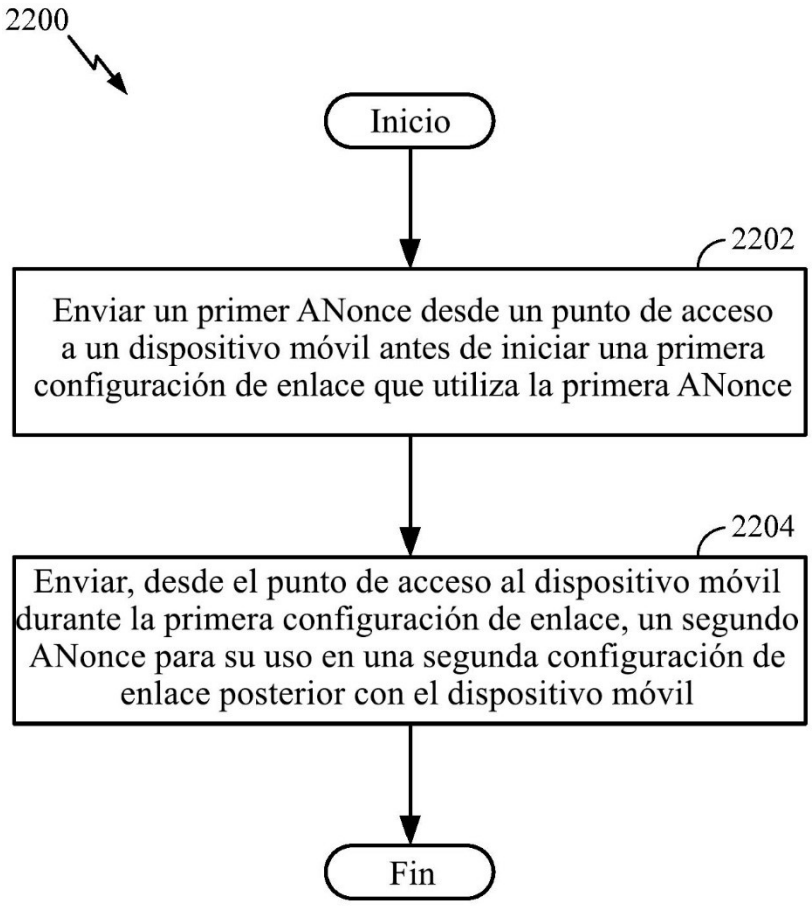
2200
Inicio
2202
Enviar un primer ANonce desde un punto de acceso a un dispositivo móvil antes de iniciar una primera configuración de enlace que utiliza la primera ANonce
2204
Enviar, desde el punto de acceso al dispositivo móvil durante la primera configuración de enlace, un segundo ANonce para su uso en una segunda configuración de enlace posterior con el dispositivo móvil
Fin

FIG. 22

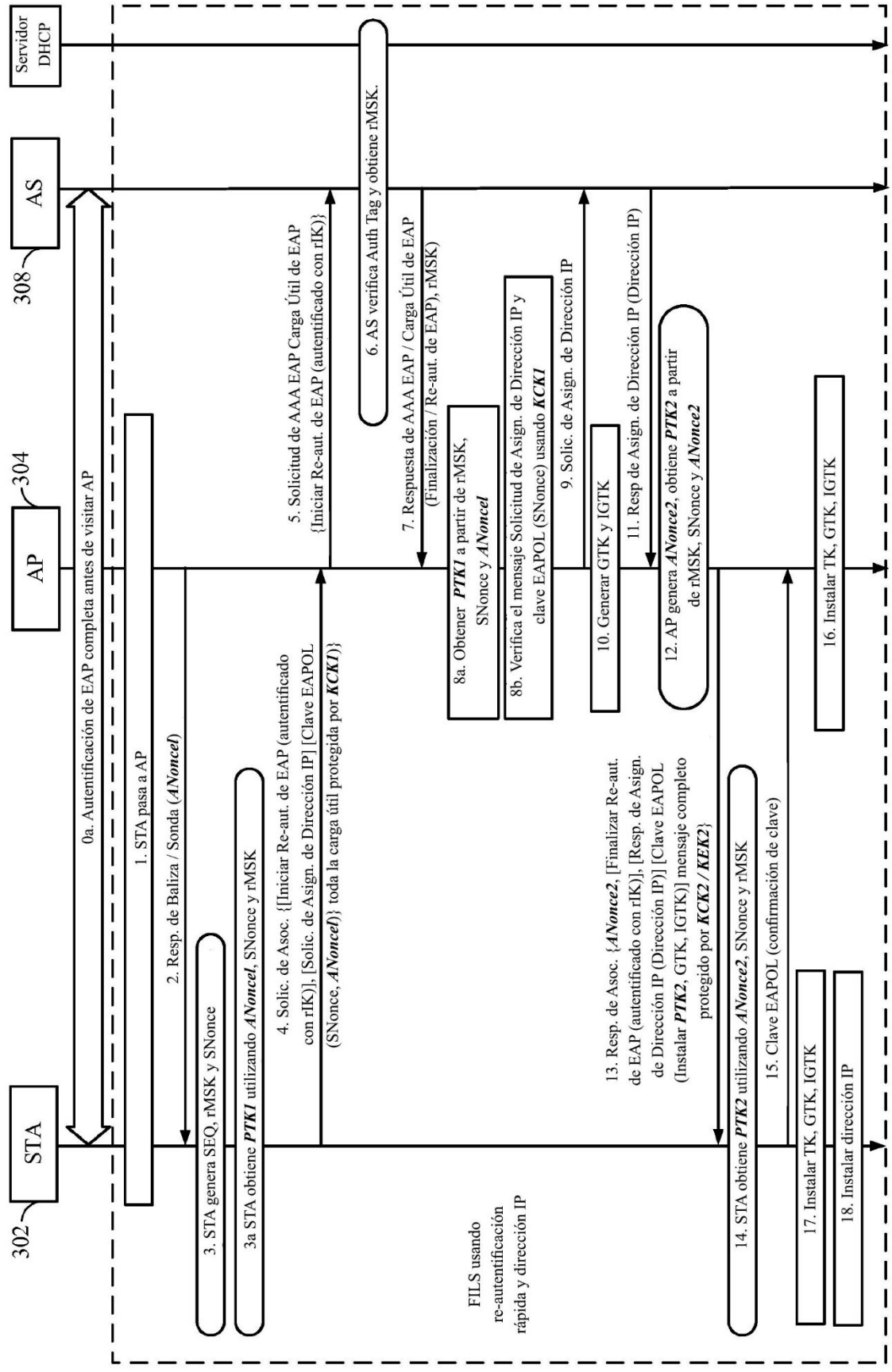
302
STA
AP
304
308
AS
Servidor DHCP
0a. Autentificación de EAP completa antes de visitar AP
1. STA pasa a AP
2. Resp. de Baliza / Sonda (ANoncel)
3. STA genera SEQ, rMSK y SNonce
3a STA obtiene PTK1 utilizando ANoncel, SNonce y rMSK
4. Solic. de Asoc. {[Iniciar Re-aut. de EAP (autentificado con rIK)], [Solic. de Asign. de Dirección IP] [Clave EAPOL (SNonce, ANoncel)} toda la carga útil protegida por KCK1)}
5. Solicitud de AAA EAP Carga Útil de EAP {Iniciar Re-aut. de EAP (autentificado con rIK)}
6. AS verifica Auth Tag y obtiene rMSK.
7. Respuesta de AAA EAP / Carga Útil de EAP (Finalización / Re-aut. de EAP), rMSK)
8a. Obtener PTK1 a partir de rMSK, SNonce y ANoncel
8b. Verifica el mensaje Solicitud de Asign. de Dirección IP y clave EAPOL (SNonce) usando KCK1
9. Solic. de Asign. de Dirección IP
10. Generar GTK y IGTK
11. Resp de Asign. de Dirección IP (Dirección IP)
12. AP genera ANonce2, obtiene PTK2 a partir de rMSK, SNonce y ANonce2
13. Resp. de Asoc. {ANonce2, [Finalizar Re-aut. de EAP (autentificado con rIK)], [Resp. de Asign. de Dirección IP (Dirección IP)] [Clave EAPOL (Instalar PTK2, GTK, IGTK)] mensaje completo protegido por KCK2 / KEK2}
14. STA obtiene PTK2 utilizando ANonce2, SNonce y rMSK
15. Clave EAPOL (confirmación de clave)
16. Instalar TK, GTK, IGTK
17. Instalar TK, GTK, IGTK
18. Instalar dirección IP
FILS usando re-autentificación rápida y dirección IP

FIG. 23

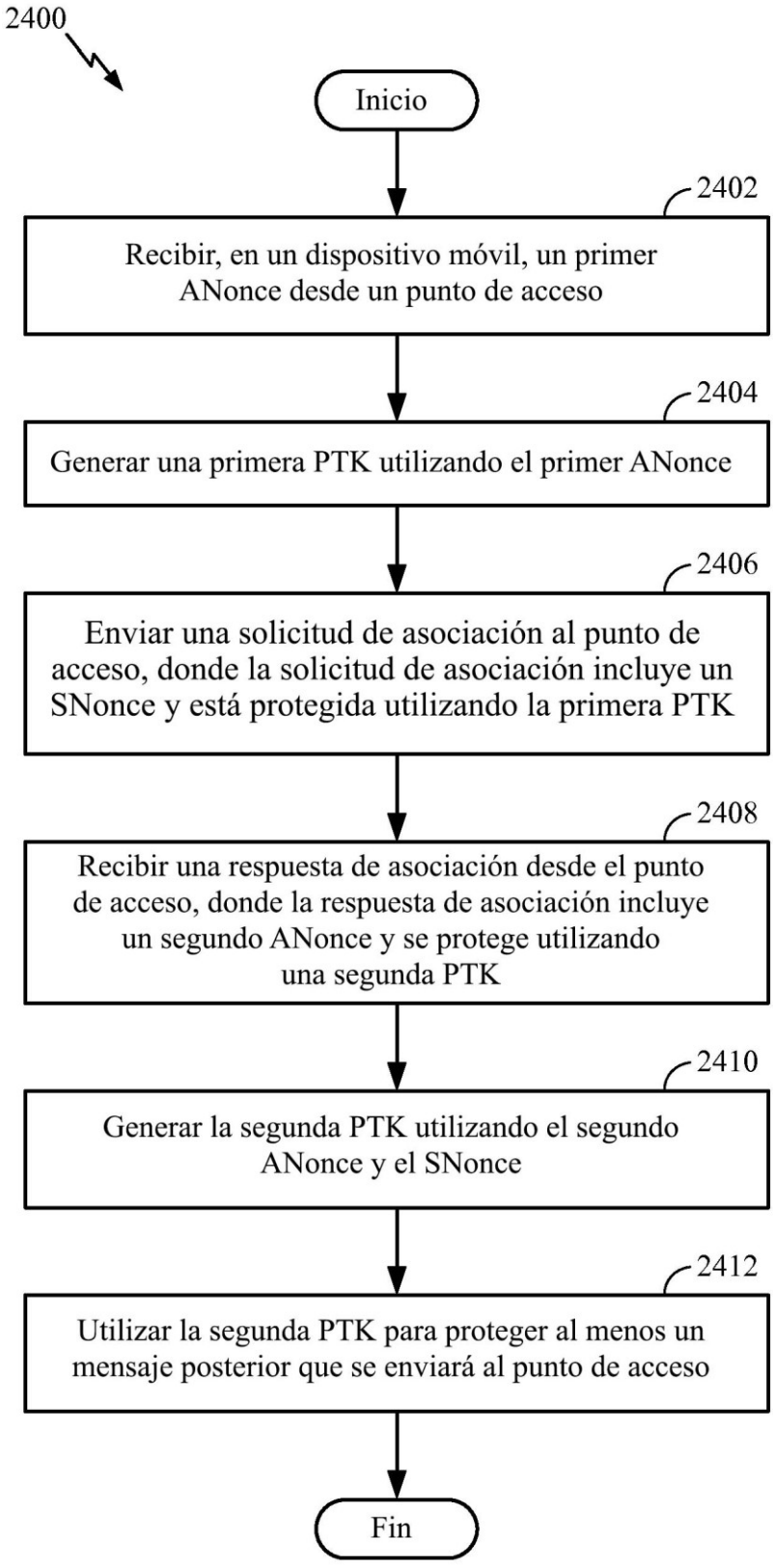
2400
Inicio
2402
Recibir, en un dispositivo móvil, un primer ANonce desde un punto de acceso
2404
Generar una primera PTK utilizando el primer ANonce
2406
Enviar una solicitud de asociación al punto de acceso, donde la solicitud de asociación incluye un SNonce y está protegida utilizando la primera PTK
2408
Recibir una respuesta de asociación desde el punto de acceso, donde la respuesta de asociación incluye un segundo ANonce y se protege utilizando una segunda PTK
2410
Generar la segunda PTK utilizando el segundo ANonce y el SNonce
2412
Utilizar la segunda PTK para proteger al menos un mensaje posterior que se enviará al punto de acceso
Fin

FIG. 24

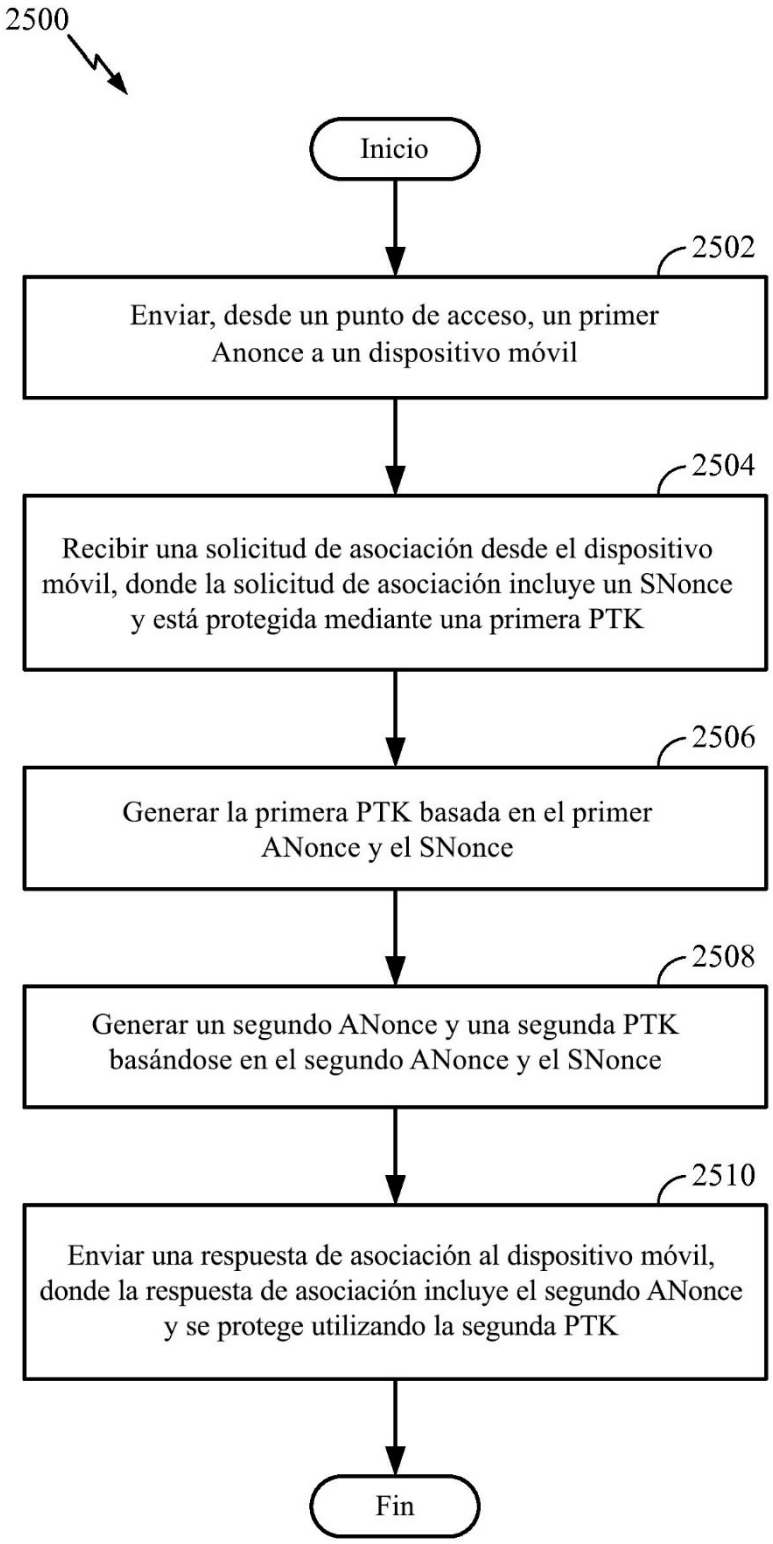
2500
Inicio
2502
Enviar, desde un punto de acceso, un primer Anonce a un dispositivo móvil
2504
Recibir una solicitud de asociación desde el dispositivo móvil, donde la solicitud de asociación incluye un SNonce y está protegida mediante una primera PTK
2506
Generar la primera PTK basada en el primer ANonce y el SNonce
2508
Generar un segundo ANonce y una segunda PTK basándose en el segundo ANonce y el SNonce
2510
Enviar una respuesta de asociación al dispositivo móvil, donde la respuesta de asociación incluye el segundo ANonce y se protege utilizando la segunda PTK
Fin

FIG. 25

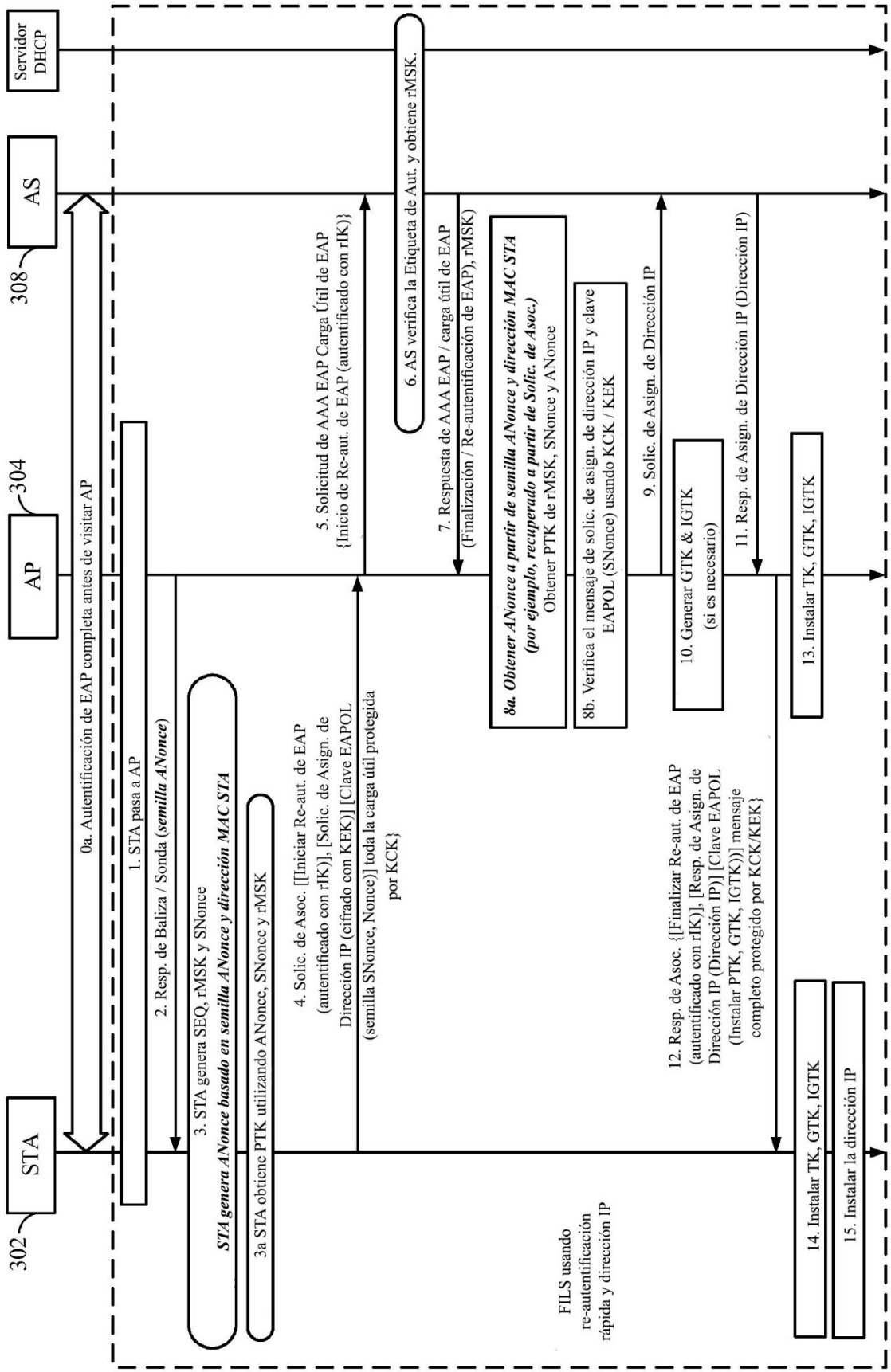
302
STA
304
AP
308
AS
Servidor DHCP
0a. Autentificación de EAP completa antes de visitar AP
1. STA pasa a AP
2. Resp. de Baliza / Sonda (semilla ANonce)
3. STA genera SEQ, rMSK y SNonce
STA genera ANonce basado en semilla ANonce y dirección MAC STA
3a STA obtiene PTK utilizando ANonce, SNonce y rMSK
4. Solic. de Asoc. [[Iniciar Re-aut. de EAP (autentificado con rIK)], [Solic. de Asign. de Dirección IP (cifrado con KEK)] [Clave EAPOL (semilla SNonce, Nonce)] toda la carga útil protegida por KCK}
5. Solicitud de AAA EAP Carga Útil de EAP {Inicio de Re-aut. de EAP (autentificado con rIK)}
6. AS verifica la Etiqueta de Aut. y obtiene rMSK.
7. Respuesta de AAA EAP / carga útil de EAP (Finalización / Re-autentificación de EAP), rMSK)
8a. Obtener ANonce a partir de semilla ANonce y dirección MAC STA (por ejemplo, recuperado a partir de Solic. de Asoc.)
Obtener PTK de rMSK, SNonce y ANonce
8b. Verifica el mensaje de solic. de asign. de dirección IP y clave EAPOL (SNonce) usando KCK / KEK
9. Solic. de Asign. de Dirección IP
10. Generar GTK & IGTK (si es necesario)
11. Resp. de Asign. de Dirección IP (Dirección IP)
12. Resp. de Asoc. {[Finalizar Re-aut. de EAP (autentificado con rIK)], [Resp. de Asign. de Dirección IP (Dirección IP)] [Clave EAPOL (Instalar PTK, GTK, IGTK)] mensaje completo protegido por KCK/KEK}
13. Instalar TK, GTK, IGTK
14. Instalar TK, GTK, IGTK
15. Instalar la dirección IP
FILS usando re-autentificación rápida y dirección IP

FIG. 26

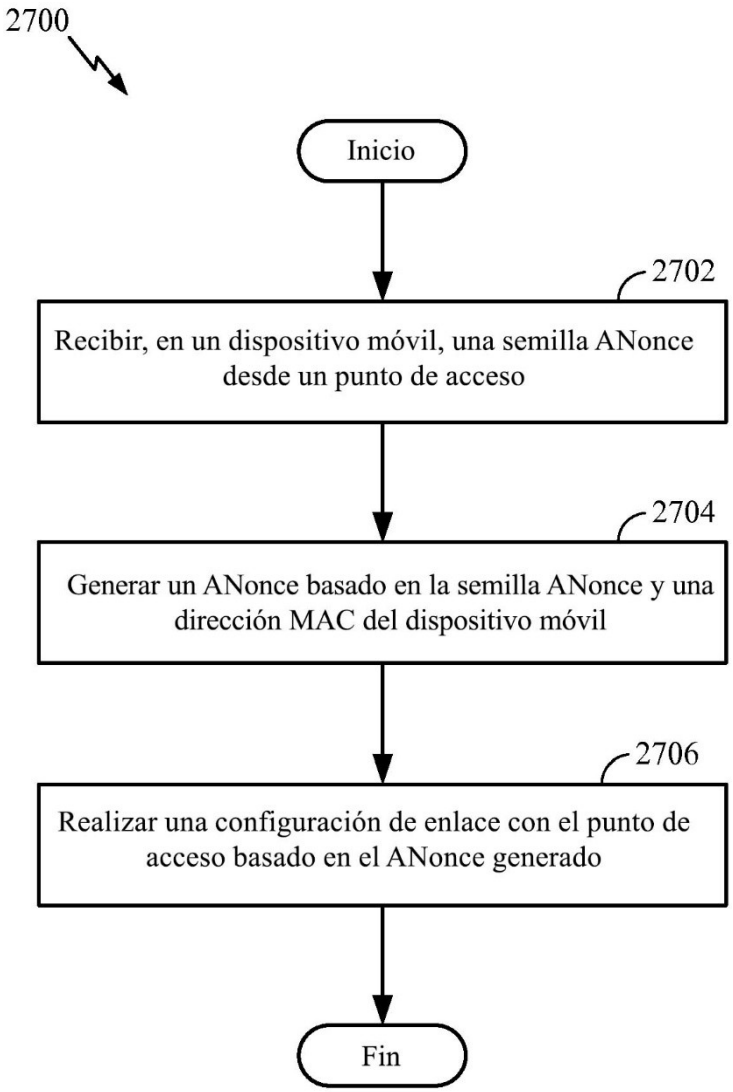
2700
Inicio
2702
Recibir, en un dispositivo móvil, una semilla ANonce desde un punto de acceso
2704
Generar un ANonce basado en la semilla ANonce y una dirección MAC del dispositivo móvil
2706
Realizar una configuración de enlace con el punto de acceso basado en el ANonce generado
Fin

FIG. 27

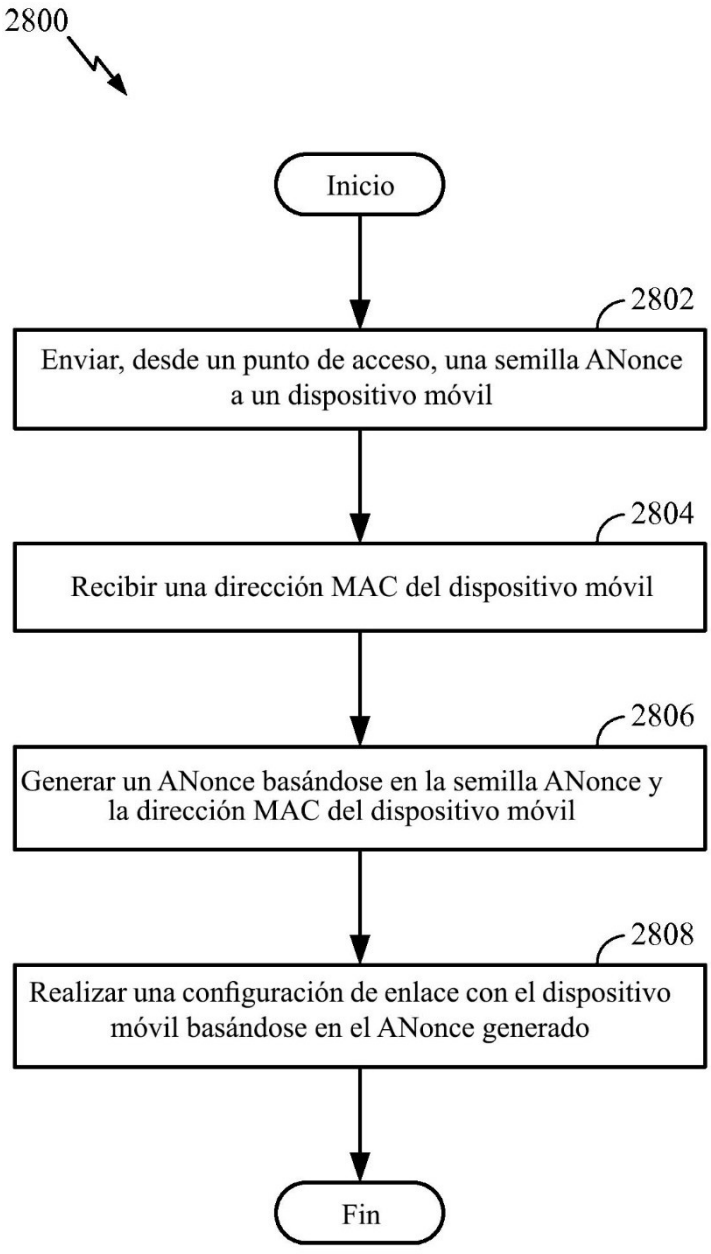
2800
Inicio
2802
Enviar, desde un punto de acceso, una semilla ANonce a un dispositivo móvil
2804
Recibir una dirección MAC del dispositivo móvil
2806
Generar un ANonce basándose en la semilla ANonce y la dirección MAC del dispositivo móvil
2808
Realizar una configuración de enlace con el dispositivo móvil basándose en el ANonce generado
Fin

FIG. 28