(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 564 484**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.10.2011 E 11846361 (1)**

(97) Fecha y número de publicación de la concesión europea: **30.12.2015 EP 2651156**

(54) Título: **Método de autenticación 802.1X centralizado, dispositivo y sistema de red de área local inalámbrica**

(30) Prioridad:

09.12.2010 CN 201010581115

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.03.2016

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

LIU, GUOPING

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método de autenticación 802.1X centralizado, dispositivo y sistema de red de área local inalámbrica

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de tecnologías de comunicaciones y en particular, a un método, un aparato y un sistema para la autenticación centralizada según el protocolo 802.1X en una red de área local inalámbrica.

ANTECEDENTES DE LA INVENCIÓN

La estructura básica de una red de área local inalámbrica, (WLAN, Wireless Local Area Network) definida en IEEE (Institute of Electrical and Electronics Engineers, Institute of Electronical and Electronics Engineers de los Estados Unidos) 802.1X puede ilustrarse en la Figura 1, en donde una estación (STA, Station) se refiere a un dispositivo terminal que tiene una interfaz de red de área local inalámbrica y un punto de acceso (AP, Access Point) es equivalente a una estación base de una red móvil y es principalmente responsable de la puesta en práctica de la comunicación entre las estaciones STAs o entre una estación STA y un dispositivo pertinente de una red cableada. Múltiples estaciones STAs pueden acceder al mismo punto de acceso AP. Las estaciones STAs asociadas con el mismo AP constituyen un conjunto de servicio básico (BSS, Basic service set). Un sistema de distribución (DS, Distribution System) se utiliza para formar una red de área local amplia entre diferentes conjuntos BSSs así como entre un conjunto BSS y una red de área local cableada. Un dispositivo de portal (portal) es un punto lógico para proporcionar datos mediante un reenvío entre un sistema DS y una red de área local cableada.

En un sistema WLAN, identificadores de conjunto de servicios (SSID, Service Set Identifier) se utilizar para distinguir diferentes redes de área local inalámbricas. Cuando diferentes conjuntos BSSs (que se pueden identificar utilizando identificadores BSSIDs) forman una red de área local amplia mediante un sistema DS, teniendo el mismo identificador SSID.

Actualmente, un mecanismo de seguridad de acceso protegido de WI-FI (WPA, WI-FI Protected Access), recomendado por la alianza de certificación de prioridad inalámbrica (WI-FI, wireless fidelity) se aplica ampliamente en una red WLAN. La versión de empresa de WPA (generalmente referida a diversas versiones de empresa de WPA) se pone en práctica sobre la base del protocolo de autenticación 802.1X. Una estructura de red de la autenticación según el protocolo 802.1X puede dividirse en tres partes, incluyendo una parte de aplicación de autenticación (es decir, una entidad de acceso de puerto de usuario (equipo de usuario (UE, User Equipment) en forma abreviada y en una red WLAN, un equipo de usuario UE puede referirse como una estación STA)), un sistema de autenticación (Authenticator system) (es decir, una entidad de autenticación (AE, Authentication Entity)) y un servidor de autenticación (AS, Authenticator server system).

Por defecto, una entidad AE solamente permite un mensaje de autenticación de un equipo UE para transmitirse al principio y la entidad AE permite un mensaje de servicio del equipo UE para transmitir solamente después de que se haya realizado la autenticación del UE. En una red WLAN, una entidad AS es un servidor de servicio de usuario de marcación de autenticación distante (Radius, Remote Authentication Dial In User Service), la entidad AE suele corresponder a un punto de acceso AP y el equipo UE es una estación STA.

En un proceso de autenticación, un mensaje de autenticación se transmite entre una estación STA y un punto de acceso AP. Existe un proceso de asociación entre la estación STA y el punto de acceso AP antes de que la autenticación se inicie en una red WLAN. Por lo tanto, la estación STA y el punto de acceso AP tienen ambos conocimiento de una dirección de control de acceso al medio (MAC, Media Access Control) de interfaz de aire (tal como un identificador BSSID) de un extremo homólogo antes de la autenticación. Por lo tanto, el protocolo IEEE 802.1X especifica que en una red WLAN, todos los mensajes de autenticación del denominado Protocolo de Autenticación Extensivo (EAP, Extensive Authentication Protocol) (incluyendo un primer mensaje) de un equipo UE debe utilizar direcciones de unidifusión.

En una red WLAN especificada en el protocolo IEEE 802.1X, un requisito previo para todos los mensajes de autenticación EAP para utilizar direcciones de unidifusión es que una entidad AE debe ser un dispositivo de punto de acceso AP (un equipo UE puede tener conocimiento de la dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso AP en un proceso de asociación con el AP). Una red WLAN en un escenario operativo tal como una vivienda o una pequeña empresa puede satisfacer esta condición puesto que la cantidad de puntos de acceso APs está limitada en los escenarios operativos y no se requiere mucho trabajo para configurar cada punto de acceso AP como una entidad AE. Este modo de desarrollo de autenticación puede referirse como un desarrollo de autenticación distribuida.

A medida que se desarrollan tecnologías, se desarrolla un gran número de redes WLAN amplias adecuadas para una gran empresa u operador, y una red WLAN amplia tiene un gran número de puntos de acceso APs. Para facilitar la carga de gestión, se suele utilizar la gestión de redes de puntos de acceso AP actualmente. En este caso, un

dispositivo de entidad AE puede desarrollarse en un controlador de acceso (AC, Access controller) o desarrollarse en un dispositivo de pasarela de control multiservicio (MSCG, Multi-service control Gateway) en el controlador AC. El modo de desarrollo de la autenticación de despliegue operativo de un dispositivo de entidad AE en un dispositivo tal como un controlador AC o un MSCG, en una forma centralizada, puede referirse como desarrollo de autenticación centralizada.

Una entidad AE en el desarrollo de autenticación centralizada no es un dispositivo de punto de acceso AP; por lo tanto, un equipo UE no puede tener conocimiento de una dirección MAC de la entidad AE antes de la autenticación. Sin embargo, el protocolo IEEE 802.1X especifica que todos los mensajes de autenticación EAP (incluyendo un primer mensaje) de un equipo de usuario UE deben utilizar direcciones de unidifusión. En tal caso, la autenticación no puede realizarse en conformidad con el mecanismo existente.

El documento US 2010/182983 A1 da a conocer un sistema de red de área local inalámbrica que comprende un controlador de red WLAN y una pluralidad de puntos de acceso. El controlador de red WLAN está configurado para realizar una o más funciones de control de red para el beneficio de la pluralidad de puntos de acceso. Las funciones de control de la red pueden seleccionarse a partir de la gestión y operación, autenticación de clientes, movilidad y administración por usuario.

El documento “MENEZES, VANSTONE, OORSCHOT: “Manual de Criptografía aplicada”, 1997, CRC PRESS LLC., USA” da a conocer una estructura para autenticación, y proporciona un método de autenticación basado en esta estructura.

SUMARIO DE LA INVENCIÓN

Formas de realización de la presente invención dan a conocer un método, un aparato y un sistema para autenticación centralizada del protocolo 802.1X en una red de área local inalámbrica, con lo que se pone en práctica la autenticación centralizada de 802.1X para un equipo de usuario UE en una red de área local inalámbrica.

Con el fin de resolver los problemas técnicos anteriores, las formas de realización de la presente invención dan a conocer las soluciones técnicas siguientes.

Un método para la autenticación centralizada de 802.1X en una red de área local inalámbrica, en donde la red de área local inalámbrica comprende una entidad de autenticación, AE, un punto de acceso, AP y al menos un equipo de usuario UE, la entidad AE está conectada a al menos un equipo UE por intermedio del punto de acceso AP, caracterizado por cuanto que el método comprende:

la generación, por el punto de acceso AP, de un mensaje de inicio de autenticación de protocolo de autenticación extensiva, un mensaje EAPOL-Start, después de que un equipo UE se asocie con el punto de acceso AP, en donde una dirección de destino del mensaje EAPOL-Start es una dirección de multidifusión de una Entidad de Acceso de Puerto, PAE o un Control de Acceso a Medio, MAC, de la entidad AE y una dirección origen del mensaje EAPOL-Start es una dirección MAC del equipo de usuario UE asociado;

el envío, por el punto de acceso AP, del mensaje EAPOL-Start;

la recepción, por el punto de acceso AP, de un primer mensaje de autenticación EAP procedente de la entidad AE; en donde una dirección origen del primer mensaje de autenticación EAP es la dirección MAC de la entidad AE y una dirección de destino del primer mensaje de autenticación EAP es la dirección MAC del equipo de usuario UE asociado; y

la modificación, por el punto de acceso AP, de la dirección origen del primer mensaje de autenticación EAP para ser una dirección MAC correspondiente a una interfaz de aire del punto de acceso AP; y

el reenvío, por el punto de acceso AP, del mensaje de autenticación EAP modificado al equipo de usuario UE asociado con el fin de que el equipo UE asociado utilice el punto de acceso AP como una entidad AE para continuar la autenticación EAP.

Un dispositivo de punto de acceso AP, que comprende:

un módulo de generación, configurado para generar un mensaje de inicio de autenticación de protocolo de autenticación extensiva, un mensaje EAPOL-Start, después de que el equipo UE se asocie con el dispositivo AP; en donde una dirección de destino del mensaje EAPOL-Start es una dirección de multidifusión de una Entidad de Acceso de Puerto, PAE o un Control de Acceso a Medio, MAC de una entidad de autenticación, AE y una dirección origen del mensaje EAPOL-Start es una dirección MAC del equipo de usuario UE asociado;

un módulo de envío, configurado para enviar el mensaje EAPOL-Start;

un módulo de recepción, configurado para recibir un primer mensaje de autenticación EAP desde la entidad AE; en donde la dirección origen del primer mensaje de autenticación EAP es la dirección MAC de la entidad AE y una dirección de destino del primer mensaje de autenticación EAP es la dirección MAC del equipo UE asociado;

un módulo de modificación y de reenvío, configurado para modificar la dirección origen del primer mensaje de autenticación EAP para ser una dirección MAC correspondiente a una interfaz de aire del punto de acceso AP; y reenviar el mensaje de autenticación EAP modificado al equipo UE asociado con el fin de que el equipo UE asociado utilice el punto de acceso AP como una entidad AE para continuar la autenticación EAP.

Un sistema para autenticación centralizada 802.1X en una red de área local inalámbrica, en donde la red de área local inalámbrica comprende un punto de acceso en conformidad con cualquiera de las reivindicaciones 5 a 7, una entidad de autenticación, AE, y al menos un equipo de usuario, UE, estando la entidad AE conectada a al menos un equipo UE por intermedio del punto de acceso.

En conformidad con la descripción anterior, en una solución técnica dada a conocer por la forma de realización de la presente invención, después de la recepción, desde un equipo UE, de un mensaje de inicio de autenticación EAP cuya dirección de destino es una dirección MAC correspondiente a una interfaz de aire del punto de acceso, un punto de acceso en el desarrollo de autenticación centralizada modifica la dirección de destino del mensaje para ser una dirección MAC de una entidad de autenticación, y reenvía el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar la entidad de autenticación en lugar de detenerse en el punto de acceso, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y poner en práctica la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite al equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar el programa de autenticación que se establece en el UE y está basado en el mecanismo del protocolo IEEE 802.1X.

En otra solución técnica dada a conocer por las formas de realización de la presente invención, un punto de acceso en un desarrollo de autenticación centralizada genera y envía un mensaje de inicio de autenticación EAP cuya dirección origen es una dirección MAC de un equipo UE y cuya dirección de destino es una dirección MAC de una entidad AE, para actuar como un dispositivo proxy para el equipo UE para iniciar un proceso de autenticación de acceso, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar una entidad de autenticación, con el fin de iniciar un proceso de autenticación del acceso para el equipo UE y poner en práctica la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite a un equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar el programa de autenticación que se establece en el equipo UE y está basado en el mecanismo del protocolo IEEE 802.1X.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en las formas de realización de la presente invención o en la técnica anterior con mayor claridad, a continuación se introducen brevemente los dibujos adjuntos requeridos para describir las formas de realización o la técnica anterior. Evidentemente, los dibujos adjuntos en la siguiente descripción ilustran simplemente algunas formas de realización de la presente invención y los expertos ordinarios en esta técnica pueden derivar todavía otros dibujos a partir de los dibujos adjuntos sin necesidad de esfuerzos creativos.

La Figura 1 es un diagrama esquemático de una estructura básica de una red WLAN definida en 802.1X;

La Figura 2 es un diagrama esquemático de una topología de una red de autenticación centralizada en desarrollo en conformidad con una forma de realización de la presente invención,

La Figura 3 es un diagrama de flujo esquemático de un método para la autenticación centralizada 802.1X en una red de área local inalámbrica en conformidad con la forma de realización 1 de la presente invención,

La Figura 4 es un diagrama de flujo esquemático de un método para la autenticación centralizada 802.1X en una red de área local inalámbrica en conformidad con la forma de realización 2 de la presente invención;

La Figura 5 es un diagrama de flujo esquemático de un método para la autenticación centralizada 802.1X en una red de área local inalámbrica en conformidad con la forma de realización 3 de la presente invención;

La Figura 6 es un diagrama de flujo esquemático de un método para la autenticación centralizada 802.1X en una red de área local inalámbrica en conformidad con la forma de realización 4 de la presente invención;

La Figura 7 es un diagrama esquemático de un punto de acceso en conformidad con una forma de realización de la presente invención;

La Figura 8 es un diagrama esquemático de otro punto de acceso en conformidad con una forma de realización de la presente invención;

La Figura 9 es un diagrama esquemático de otro punto de acceso en conformidad con una forma de realización de la presente invención;

La Figura 10 es un diagrama esquemático de un sistema para la autenticación centralizada 802.1X en una red de área local inalámbrica en conformidad con una forma de realización de la presente invención; y

La Figura 11 es un diagrama esquemático de otro sistema para la autenticación centralizada 802.1X en una red de área local inalámbrica en conformidad con una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN DE LA INVENCIÓN

Formas de realización de la presente invención dan a conocer un método, un aparato y un sistema para autenticación centralizada 802.1X en una red de área local inalámbrica.

Para hacer más comprensibles los objetivos, las características y las ventajas de la presente invención, a continuación se describe, de forma clara y completa, las soluciones técnicas en las formas de realización de la presente invención haciendo referencia a los dibujos adjuntos en dichas formas de realización de la presente invención. Evidentemente, las formas de realización descritas son simplemente una parte y no la totalidad de las formas de realización de la presente invención. Todas las demás formas de realización obtenidas por expertos en esta técnica sobre la base de las formas de realización de la presente invención, sin necesidad de esfuerzos creativos, caerán dentro del alcance de protección de la presente invención.

Haciendo referencia a la Figura 2, se ilustra un diagrama esquemático de una topología de una red de autenticación centralizada en desarrollo en conformidad con una forma de realización de la presente invención. Múltiples equipos de usuario UEs pueden asociarse con un solo punto de acceso AP; múltiples puntos de acceso APs se conectan luego a un controlador de acceso AC; y un dispositivo de entidad AE puede desarrollarse en el controlador AC o desarrollarse en un dispositivo de pasarela de control multiservicio MSCG en el controlador AC. La Figura 2 ilustra un escenario operativo en donde un dispositivo de entidad AE se desarrolla en un controlador AC. El dispositivo de entidad AE está asociado con un AS para formar un desarrollo de autenticación centralizada. Las soluciones técnicas en conformidad con las formas de realización de la presente invención pueden ponerse en práctica concretamente sobre la base de una red de autenticación de una estructura de topología ilustrada en la Figura 2 o una red de autenticación de una estructura de desarrollo centralizada similar.

A continuación se proporciona una descripción detallada de lo que antecede.

Forma de realización 1

En una forma de realización que ilustra un método para la autenticación centralizada 802.1X es una red de área local inalámbrica en conformidad con la presente invención, una red de área local inalámbrica incluye una entidad AE, un punto de acceso AP y al menos un equipo de usuario UE, en donde la entidad AE está conectada a al menos un equipo UE por intermedio del punto de acceso AP y el método puede incluir: la recepción, por el punto de acceso AP de un mensaje de inicio de autenticación EAP enviado por el equipo UE, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección de control de acceso al medio (MAC, Media Access Control) correspondiente a una interfaz de aire del punto de acceso AP y su dirección origen es una dirección MAC del equipo UE; la modificación de la dirección de destino del mensaje de inicio de autenticación EAP para ser una dirección de multidifusión de una entidad de acceso de puerto (PAE, Port Access Entity) o una dirección MAC de la entidad AE; y el reenvío del mensaje de inicio de autenticación EAP cuya dirección de destino es modificada, de modo que la entidad AE inicie la autenticación de acceso para el equipo UE en conformidad con el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada.

Haciendo referencia a la Figura 3 pueden incluirse las etapas específicas siguientes:

310. Un punto de acceso AP recibe un mensaje de inicio de autenticación EAP enviado por un equipo UE, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección MAC correspondiente a una interfaz de aire del punto de acceso AP y su dirección origen es una dirección MAC del equipo UE.

En un escenario operativo de aplicación, un equipo UE puede iniciar una demanda de autenticación enviando un mensaje de inicio de autenticación EAP (mensaje EAPOL-Start), con lo que se demanda a un lado de red la realización de la autenticación de acceso.

Antes de que el equipo UE inicie la autenticación, existe un proceso de asociación con el punto de acceso AP y el equipo UE y el punto de acceso AP ambos tienen conocimiento de una dirección de control de acceso al medio MAC de un extremo homólogo antes de la autenticación. Por lo tanto, el equipo UE puede enviar el mensaje de inicio de

autenticación EAP en un modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X, en donde la dirección MAC del punto de acceso AP que se incluye en el mensaje de inicio de autenticación EAP puede ser un identificador BSSID u otro identificador de distinción.

320. El punto de acceso AP modifica la dirección de destino del mensaje de inicio de autenticación EAP para ser una dirección MAC de una entidad AE o una dirección de multidifusión de una PAE.

Cuando el punto de acceso AP supervisa que la dirección de destino del mensaje de inicio de autenticación EAP recibido es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP, el punto de acceso AP no interrumpe el mensaje de inicio de autenticación EAP en este punto, sino que continúa su reenvío después de modificar su dirección de destino.

En una aplicación práctica, si la dirección MAC de la entidad AE se configura por anticipado para el punto de acceso AP, el punto de acceso AP puede modificar la dirección de destino del mensaje de inicio de autenticación EAP recibido para ser la dirección MAC de la entidad AE; si el punto de acceso AP no tiene conocimiento de la dirección MAC de la entidad AE en este momento, el punto de acceso AP puede modificar la dirección de destino del mensaje de inicio de autenticación EAP recibido para ser una dirección de multidifusión de la PAE, en donde el mensaje de inicio de autenticación EAP cuya dirección de destino es la dirección de multidifusión de la PAE puede detectarse y recibirse también por la entidad AE.

330. El punto de acceso AP reenvía el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada.

En correspondencia, la entidad AE puede recibir el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada, con lo que se tiene conocimiento de que el equipo UE demanda una autenticación de acceso; y la entidad AE puede responder en conformidad con un proceso de autenticación estándar para iniciar la autenticación de acceso para el equipo UE.

En un escenario operativo de aplicación, si el punto de acceso AP recibe, además, un mensaje de autenticación EAP (tal como un mensaje de demanda de EAP (EAP-Request message) para demandar la identidad de un equipo UE u otro mensaje) enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE, el punto de acceso AP puede modificar la dirección origen del mensaje de autenticación EAP para ser la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP y reenviar el mensaje de autenticación EAP con la dirección origen modificada al equipo UE. En este caso, puesto que la dirección origen del mensaje de autenticación EAP que se reenvía por el punto de acceso AP y se recibe por el equipo UE es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP, el equipo UE puede utilizar todavía el punto de acceso AP como una entidad AE para continuar la autenticación EAP. Si el punto de acceso AP recibe, además, un segundo mensaje de autenticación EAP enviado por el equipo UE en donde el segundo mensaje de autenticación EAP es un mensaje de autenticación (el segundo mensaje de autenticación EAP es como, a modo de ejemplo, un mensaje de respuesta de EAP (EAP-Response) que incluye una identidad de UE (ID) u otro mensaje de autenticación EAP) enviado por el equipo UE con la excepción del mensaje de inicio de autenticación EAP, una dirección de destino del segundo mensaje de autenticación EAP es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP, y su dirección origen es la dirección MAC del equipo UE, el punto de acceso AP puede modificar la dirección de destino del segundo mensaje de autenticación EAP para ser la dirección MAC de la entidad AE, y reenviar el segundo mensaje de autenticación EAP cuya dirección de destino es modificada. Dicho de otro modo, el punto de acceso AP puede modificar la dirección origen o la dirección de destino de todos los mensajes de autenticación EAP comunicados entre el equipo UE y la entidad AE, modificar la dirección de destino del mensaje de autenticación EAP procedente del UE para ser la dirección MAC de la entidad AE y modificar la dirección origen del mensaje de autenticación EAP procedente de la entidad AE para ser la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP; y el equipo UE puede considerar también al punto de acceso AP como una entidad AE para la autenticación EAP. Puesto que el equipo de usuario UE tiene conocimiento de la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP antes de la autenticación, el equipo UE puede enviar todos los mensajes de autenticación EAP en un modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

En otro escenario operativo de aplicación, si el punto de acceso AP recibe, además, un tercer mensaje de autenticación EAP (tal como un mensaje de demanda de EAP (EAP-Request message) para demandar la identidad de un equipo UE u otro mensaje) enviado por la entidad AE, en donde una dirección origen del tercer mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE, el punto de acceso AP no puede modificar la dirección origen o la dirección de destino del tercer mensaje de autenticación EAP, pero reenvía directamente el tercer mensaje de autenticación EAP al equipo UE, de modo que el equipo UE tenga conocimiento de la dirección MAC de la entidad AE a partir del tercer mensaje de autenticación EAP. En este escenario operativo, después de recibir el tercer mensaje de autenticación EAP, el equipo UE puede tener conocimiento de la dirección MAC de una entidad AE real, y puede comunicarse con la entidad AE en relación

con otros mensajes de autenticación EAP utilizando la dirección MAC aprendida de la entidad AE posteriormente, con lo que se completa la autenticación de acceso. Dicho de otro modo, el punto de acceso AP puede modificar solamente la dirección de destino del mensaje de inicio de autenticación EAP (un primer mensaje de autenticación EAP procedente del equipo de usuario UE), pero no modificar la dirección origen o la dirección de destino de un mensaje de inicio de autenticación EAP comunicado entre el equipo UE y la entidad AE posteriormente y el equipo UE puede tener conocimiento de la dirección MAC de la entidad AE en conformidad con una respuesta de la entidad AE al mensaje de inicio de autenticación EAP, de modo que el equipo UE pueda enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

Conviene señalar que el equipo de usuario UE mencionado en la forma de realización de la presente invención puede ser varios dispositivos terminales que tengan capacidad de acceso de red de área local inalámbrica, tal como un teléfono móvil y un ordenador portátil y el punto de acceso AP puede ser varios dispositivos que tengan una función de acceso inalámbrica. La solución en conformidad con la forma de realización de la presente invención implica principalmente la modificación, por la punto de acceso AP, de las direcciones origen/destino de parte o de la totalidad de los mensajes de autenticación EAP comunicados entre el equipo UE y la entidad AE, y un mensaje de señalización de autenticación comunicado entre la entidad AE y un AS puede ser el mismo o similar al de un proceso estándar. Puede entenderse que bajo la arquitectura de autenticación 802.1X, varios algoritmos de autenticación EAP pueden seleccionarse en conformidad con los requisitos, tales como un algoritmo de autenticación como EAP-PEAP (EAP-Protected Extensible Authentication Protocol, protocolo de autenticación extensible protegido por el protocolo de autenticación extensiva), EAP-SIM/AKA (EAP-Subscriber Identity Module/Authentication y key Agreement, módulo de autenticación de abonado-protocolo de autenticación extensiva y acuerdo de claves) y EAP-TLS (protocolo de autenticación extensiva-protocolo de seguridad de la capa de transporte, EAP-Transport Layer Security Protocol). Sin embargo, la autenticación bajo la arquitectura de autenticación de 802.1X no resulta afectada por diferentes algoritmos de autenticación EAP.

En conformidad con la descripción anterior, en la forma de realización, después de que un punto de acceso AP en un desarrollo de autenticación centralizada reciba, desde un equipo de usuario UE, un mensaje de inicio de autenticación EAP cuya dirección de destino es una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso AP, el punto de acceso AP modifica la dirección de destino del mensaje para ser una dirección MAC de una entidad AE y reenvía el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar la entidad AE en lugar de detenerse en el punto de acceso AP, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y realizar una autenticación 802.1X centralizada para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite al equipo UE enviar todos los mensajes de autenticación EAP en un modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo UE y sobre la base del mecanismo del protocolo IEEE 802.1X.

Forma de realización 2

En otra forma de realización se ilustra un método para la autenticación 802.1X centralizada, en una red de área local inalámbrica en conformidad con la presente invención, una red de área local inalámbrica incluye una entidad AE, un punto de acceso AP y al menos un equipo UE, en donde la entidad AE está conectada a al menos un equipo UE por intermedio del punto de acceso AP, y el método puede incluir: la generación, por el punto de acceso AP, de un mensaje de inicio de autenticación EAP, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección de multidifusión de una PAE o una dirección MAC de la entidad AE y su dirección origen es una dirección MAC del equipo UE; el envío del mensaje de inicio de autenticación EAP; la recepción de un mensaje de autenticación EAP enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE; y el reenvío del mensaje de autenticación EAP al equipo UE, de modo que el equipo UE tenga conocimiento de la dirección MAC de la entidad AE a partir del mensaje de autenticación EAP; o la modificación de la dirección origen del mensaje de autenticación EAP recibido para ser una dirección MAC correspondiente a una interfaz de aire del punto de acceso AP, y el reenvío del mensaje de autenticación EAP cuya dirección de destino se modifica para el equipo de usuario UE.

Haciendo referencia a la Figura 4, pueden incluirse las etapas específicas siguientes.

410. Un punto de acceso AP genera un mensaje de inicio de autenticación EAP, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección de multidifusión de PAE o una dirección MAC de una entidad AE y su dirección origen es una dirección MAC de un equipo de usuario UE.

En algunos escenarios operativos de aplicación, un equipo UE no inicia activamente la autenticación 802.1X después de asociarse con un punto de acceso AP, es decir, no envía activamente un mensaje EAPOL-Start. En este caso, el punto de acceso AP puede enviar un mensaje EAPOL-Start como un dispositivo proxy del equipo de usuario UE a la entidad AE, para iniciar la autenticación 802.1X.

420. El punto de acceso AP envía el mensaje de inicio de autenticación EAP.

En la forma de realización, el punto de acceso AP inicia una demanda de autenticación como un dispositivo proxy del equipo UE, para demandar a un lado de red la realización de la autenticación de acceso para el equipo UE. El punto de acceso AP genera y envía el mensaje de inicio de autenticación EAP para iniciar un proceso de autenticación de acceso del equipo UE. En una aplicación práctica, si la dirección MAC de la entidad AE está configurada para el punto de acceso AP por anticipado, una dirección de destino del mensaje de inicio de autenticación EAP generado y enviado por el punto de acceso AP es la dirección MAC de la entidad AE; si el punto de acceso AP no tiene conocimiento de la dirección MAC de la entidad AE en este momento, una dirección de destino del mensaje de inicio de autenticación EAP generado y enviado por el punto de acceso AP es una dirección de multidifusión de PAE, en donde el mensaje de inicio de autenticación EAP cuya dirección de destino es la dirección de multidifusión del PAE puede detectarse y recibirse por la entidad AE.

En correspondencia, la entidad AE puede recibir el mensaje de inicio de autenticación EAP y tener conocimiento de que el equipo UE demanda una autenticación de acceso y la entidad AE puede responder en conformidad con un proceso de autenticación estándar.

430. El punto de acceso AP recibe un mensaje de autenticación EAP enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE y si dirección de destino es la dirección MAC del equipo UE.

440. El punto de acceso AP reenvía el mensaje de autenticación EAP al equipo UE, de modo que el equipo UE tenga conocimiento de la dirección MAC de la entidad AE a partir del mensaje de autenticación EAP; o modifica la dirección origen del mensaje de autenticación EAP para ser una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso AP y reenvía el mensaje de autenticación EAP con la dirección origen modificada al equipo de usuario UE.

Después de recibir el mensaje de inicio de autenticación EAP, la entidad AE puede iniciar un proceso de autenticación de acceso para el equipo UE y comunicarse con el equipo UE sobre otros mensajes de autenticación EAP.

En un escenario operativo de aplicación, si el punto de acceso AP recibe un mensaje de autenticación EAP (tal como un mensaje de demanda de EAP (EAP-Request message) para demandar la identidad de un equipo UE u otro mensaje) enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE, el punto de acceso AP puede modificar la dirección origen del mensaje de autenticación EAP para ser la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP y reenviar el mensaje de autenticación EAP con la dirección origen modificada al equipo UE. En este caso, puesto que la dirección origen del mensaje de autenticación EAP que se reenvía por el punto de acceso AP y se recibe por el equipo UE es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP, el equipo UE puede utilizar todavía el punto de acceso AP como una entidad AE para continuar la autenticación EAP. Posteriormente, si el punto de acceso AP recibe, además, otro mensaje de autenticación EAP enviado por el equipo UE, en donde el mensaje de autenticación EAP es un mensaje de autenticación (a modo de ejemplo, un mensaje de respuesta EAP que incluye una identidad de UE (ID) u otro mensaje de autenticación EAP) enviado por el equipo UE, con la excepción de un mensaje de inicio de autenticación EAP, su dirección de destino del mensaje de autenticación EAP es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP y su dirección origen es la dirección MAC del equipo UE, el punto de acceso AP puede modificar la dirección de destino del mensaje de autenticación EAP para ser la dirección MAC de la entidad AE y reenviar el mensaje de autenticación EAP cuya dirección de destino se modifica. Dicho de otro modo, el punto de acceso AP puede modificar las direcciones origen y las direcciones de destino de todos los mensajes de autenticación EAP comunicados entre el equipo UE y la entidad AE, modificar la dirección de destino del mensaje de autenticación EAP procedente del UE para ser la dirección MAC de la entidad AE y modificar la dirección origen del mensaje de autenticación EAP procedente de la entidad AE para ser la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP; y el equipo UE puede considerar siempre al punto de acceso AP como una entidad AE para la autenticación EAP. Por lo tanto, el equipo UE puede enviar todos los mensajes de autenticación EAP en un modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

En otro escenario operativo de aplicación, posteriormente, si el punto de acceso AP recibe, además, un mensaje de autenticación EAP (tal como un mensaje de demanda de EAP para demandar la identidad de un equipo UE u otro mensaje) enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE, y su dirección de destino es la dirección MAC del equipo UE, el punto de acceso AP no puede modificar la dirección origen o la dirección de destino del mensaje de autenticación EAP procedente de la entidad AE, sino reenviar directamente el mensaje de autenticación EAP al equipo UE, de modo que el equipo UE tenga conocimiento de la dirección MAC de la entidad AE a partir del mensaje de autenticación EAP. En este escenario operativo, después de recibir el mensaje de autenticación EAP, el equipo UE puede tener conocimiento de

la dirección MAC de una entidad AE real, y puede comunicarse con la entidad AE sobre otros mensajes de autenticación EAP utilizando la dirección MAC aprendida de la entidad AE posteriormente, completando, de este modo, la autenticación de acceso. Dicho de otro modo, el punto de acceso AP actúa como un dispositivo proxy para el equipo UE para generar y enviar el mensaje de inicio de autenticación EAP (en donde la dirección de destino es la dirección de multidifusión de la PEA o la dirección MAC de la entidad AE y la dirección origen es la dirección MAC del equipo de usuario UE), para iniciar la autenticación de acceso para el equipo UE, el punto de acceso AP no puede modificar una dirección origen o una dirección de destino de un mensaje de inicio de autenticación EAP comunicado posteriormente entre el equipo UE y la entidad AE; y el equipo UE puede tener conocimiento de la dirección MAC de la entidad AE en función de una respuesta de la entidad AE al mensaje de inicio de autenticación EAP. Por lo tanto, el equipo de usuario UE puede enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

Conviene señalar que el equipo UE mencionado en la forma de realización de la presente invención puede ser varios dispositivos terminales que tienen capacidad de acceso de red de área local inalámbrica, tal como un teléfono móvil o un ordenador portátil; y el punto de acceso AP puede ser varios dispositivos que tienen una función de acceso inalámbrico. La solución en conformidad con la forma de realización de la presente invención implica principalmente un procesamiento intermedio realizado por el punto de acceso AP en parte o la totalidad de los mensajes de autenticación EAP comunicados entre el equipo UE y la entidad AE y un mensaje de señalización de autenticación comunicado entre la entidad AE y un AS puede ser el mismo o similar a un proceso estándar. Puede entenderse que bajo la arquitectura de autenticación 802.1X, varios algoritmos de autenticación EAP (a modo de ejemplo, algoritmos de autenticación tales como EAP-PEAP, EAP-SIM/AKA y EAP-TLS) pueden seleccionarse en conformidad con los requisitos. Sin embargo, la autenticación bajo la arquitectura de autenticación de 802.1X no resulta afectada por diferentes algoritmos de autenticación EAP.

En conformidad con la descripción anterior, en la forma de realización, un punto de acceso AP en desarrollo de autenticación centralizada genera y envía un mensaje de inicio de autenticación EAP cuya dirección de origen es una dirección MAC de un equipo UE y cuya dirección de destino es una dirección MAC de una entidad AE para actuar como un dispositivo proxy para el equipo UE para iniciar un proceso de autenticación de acceso, modo que el mensaje de inicio de autenticación EAP pueda alcanzar la entidad AE, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y poner en práctica la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite a un equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo de usuario UE y está basado en el mecanismo del protocolo IEEE 802.1X.

Forma de realización 3

Con el fin de ilustrar las soluciones técnicas en conformidad con las formas de realización de la presente invención con mayor claridad, la descripción detallada siguiente se proporciona principalmente utilizando un proceso de realización de autenticación de acceso para un equipo UE-1 usando un algoritmo de autenticación EAP-TLS a modo de ejemplo.

Según se ilustra en la Figura 5, pueden incluirse las etapas específicas siguientes.

501. Un equipo UE-1 envía un mensaje EAPOL-Start para iniciar la autenticación 802.1X.

Una dirección de destino del mensaje EAPOL-Start es una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire de un punto de acceso AP y su dirección origen es una dirección MAC del equipo UE-1.

502. El punto de acceso AP recibe el mensaje EAPOL-Start procedente del equipo UE-1, modifica la dirección de destino del mensaje EAPOL-Start para ser una dirección MAC de una entidad AE o una dirección multidifusión de un PAE y reenvía el mensaje EAPOL-Start cuya dirección de destino es modificada.

En una aplicación práctica, si la dirección MAC de la entidad AE está configurada para el punto de acceso AP por anticipado, el punto de acceso AP puede modificar la dirección de destino del mensaje EAPOL-Start para ser la dirección MAC de la entidad AE; si el punto de acceso AP no tiene conocimiento de la dirección MAC de la entidad AE en este momento operativo, el punto de acceso AP puede modificar la dirección de destino del mensaje EAPOL-Start para ser una dirección de multidifusión de PAE, en donde el mensaje EAPOL-Start cuya dirección de destino es la dirección de multidifusión de la PAE puede detectarse también y recibirse por la entidad AE.

503. La entidad AE recibe el mensaje EAPOL-Start cuya dirección de destino es modificada por el punto de acceso AP y reenvía un mensaje de demanda de EAP para demandar la identidad del equipo UE-1.

Una dirección origen del mensaje EAP-Request es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE-1.

504. El punto de acceso AP recibe el mensaje EAP-Request procedente de la entidad AE, modifica la dirección origen del mensaje EAP-Request para ser la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP y reenvía el mensaje de demanda de EAP con la dirección origen modificada.

505. El equipo UE-1 recibe el mensaje de demanda de EAP cuya dirección origen se modifica por el punto de acceso AP y tiene conocimiento de que el lado de la red demanda un reconocimiento de identidad y luego, el equipo UE-1 envía un mensaje de respuesta EAP (EAP-Response) al punto de acceso AP, en donde se incluye información tal como el identificador ID del equipo UE-1.

Puesto que el punto de acceso AP modifica la dirección origen del mensaje de demanda de EAP procedente de la entidad AE, el equipo UE-1 todavía considera al punto de acceso AP como la entidad AE para continuar el proceso de autenticación. Una dirección de destino del mensaje de respuesta de EAP enviado por el equipo UE-1 es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso AP y su dirección origen es la dirección MAC del equipo UE-1.

506. El punto de acceso AP recibe el mensaje de respuesta de EAP procedente del equipo UE-1, modifica la dirección de destino del mensaje de respuesta de EAP para ser la dirección MAC de la entidad AE y reenvía el mensaje de respuesta de EAP cuya dirección de destino es modificada a la entidad AE.

507. La entidad AE envía un mensaje EAP over Radius a un AS, en donde el mensaje de respuesta de EAP y el identificador ID de identidad del equipo UE-1 se incluyen en el mensaje EAP over Radius.

508. El AS identifica el equipo UE-1 y envía un mensaje de demanda de EAP (TLS Start) a la entidad AE, que indica que un algoritmo de autenticación EAP es EAP-TLS, para iniciar la autenticación de EAP. Si el AS selecciona otro algoritmo de autenticación EAP, el mensaje de demanda de EAP (TLS Start) puede indicar, en correspondencia un algoritmo correspondiente.

509. La entidad AE transmite el mensaje TLS Start al equipo UE-1 por intermedio del punto de acceso AP.

510. El equipo UE-1 envía un mensaje TLS client_hello a la entidad AE por intermedio del punto de acceso AP para dar respuesta al mensaje TLS Start.

511. La entidad AE transmite el mensaje TLS client_hello al AS.

512. El AS envía un mensaje TLS server_hello a la entidad AE, en donde el mensaje puede incluir un certificado AS, información de intercambio de claves y un conjunto de encriptación de seguridad que soportar por el AS y demanda un certificado del equipo UE-1.

513. La entidad AE transmite el mensaje TLS server_hello al equipo UE-1 por intermedio del punto de acceso AP.

514. El equipo UE-1 verifica el certificado de AS y envía un mensaje que incluye un resultado de la autenticación, un certificado del equipo UE-1, información de intercambio de claves y un conjunto de encriptación de seguridad soportado por el equipo UE-1 a la entidad AE por intermedio del punto de acceso AP.

515. La entidad AE transmite el mensaje al AS.

516. Después de la autenticación operativamente satisfactoria, el AS envía un mensaje que incluye un conjunto de encriptación de seguridad seleccionado por el AS para la entidad AE.

517. La entidad AE transmite el mensaje al equipo UE-1 por intermedio del punto de acceso AP.

518. El equipo UE-1 envía un mensaje de respuesta de EAP a la entidad AE por intermedio del punto de acceso AP.

519. La entidad AE transmite el mensaje de respuesta de EAP al AS.

520. El AS envía un mensaje de éxito operativo de EAP (EAP-Success) a la entidad AE, indicando que la autenticación es operativamente satisfactoria.

521. La entidad AE transmite el mensaje de éxito operativo de EAP al equipo UE-1 por intermedio del punto de acceso AP, de modo que el equipo UE-1 tenga conocimiento de que la autenticación es operativamente satisfactoria.

Conviene señalar que en la etapa 504, si después de recibir el mensaje de demanda de AP procedente de la entidad AE, el punto de acceso AP no modifica la dirección origen del mensaje (la dirección MAC de la entidad AE), pero reenvía directamente el mensaje de demanda de AP al equipo UE-1, de modo que el equipo UE-1 pueda tener

conocimiento de la dirección MAC de la entidad AE a partir del mensaje de autenticación EAP, el equipo UE-1 puede obtener la dirección MAC de la entidad AE y posteriormente, el equipo UE-1 puede comunicarse con la entidad AE sobre otros mensajes de autenticación EAP utilizando la dirección MAC aprendida de la entidad AE para completar la autenticación de acceso. Dicho de otro modo, el punto de acceso AP solamente puede modificar la dirección de destino del mensaje EAPOL-Start desde el equipo UE-1, pero no modificar la dirección origen o la dirección de destino de un mensaje de autenticación EAP comunicado entre el equipo UE-1 y la entidad AE con posterioridad; y el equipo UE-1 puede tener conocimiento de la dirección MAC de la entidad AE en función de una respuesta de la entidad AE al mensaje de inicio de autenticación EAP, de modo que el equipo UE-1 pueda enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X. Por supuesto, el mensaje over RADIUS comunicado entre la entidad AE y el AS no necesita modificarse.

Conviene señalar que la forma de realización se describe tomando principalmente un proceso de realización de la autenticación de acceso para el equipo UE-1 sobre la base de un algoritmo de autenticación de EAP-TLS, a modo de ejemplo. Por supuesto, un algoritmo de autenticación tal como EAP-PEAP o EAP-SIM/AKA puede seleccionarse también para realizar la autenticación de acceso para el equipo UE-1, en donde un proceso de aplicación es el mismo y por ello no se repiten aquí sus detalles.

En conformidad con la descripción que antecede, en la forma de realización, la autenticación centralizada 802.1X en una red de área local inalámbrica se pone en práctica detectando y retransmitiendo un mensaje EAPOL mediante un punto de acceso AP en un desarrollo de autenticación centralizada. Después de la recepción, desde un equipo UE de un mensaje de inicio de autenticación EAP cuya dirección de destino es una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso AP, el punto de acceso AP modifica la dirección de destino del mensaje para ser una dirección MAC de una entidad AE, y reenvía el mensaje de inicio de autenticación EAP cuya dirección de destino se modifica, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar la entidad AE en lugar de detenerse en el punto de acceso AP, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y realizar la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite al equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo UE y está basado en el mecanismo del protocolo IEEE 802.1X.

Forma de realización 4

Con el fin de ilustrar las soluciones técnicas en conformidad con las formas de realización de la presente invención con mayor claridad, un proceso de realización de autenticación de acceso para un equipo UE-1 sobre la base de un algoritmo de autenticación de EAP-TLS se toma, a modo de ejemplo, para una descripción detallada a continuación. La forma de realización utiliza un ejemplo en donde un punto de acceso AP actúa como un dispositivo proxy de un equipo UE-1 para iniciar una autenticación de acceso.

Según se ilustra en la Figura 6, pueden incluirse las etapas específicas siguientes.

601. Un punto de acceso AP genera y envía un mensaje EAPOL-Start.

Una dirección de destino del mensaje EAPOL-Start es una dirección MAC (tal como un identificador BSSID) de una entidad AE o una dirección de multidifusión de una PAE y su dirección origen es una dirección MAC de un equipo UE-1.

En algunos escenarios operativos de aplicación, un equipo UE-1 no inicia activamente una autenticación 802.1X después de asociarse con un punto de acceso AP. Es decir, no envía activamente un mensaje EAPOL-Start. En este caso, el punto de acceso AP puede enviar un mensaje EAPOL-Start como un dispositivo proxy del equipo UE-1 a la entidad AE, para iniciar una autenticación 802.1X.

En una aplicación práctica, si la dirección MAC de la entidad AE está configurada para el punto de acceso AP por anticipado, el punto de acceso AP puede establecer la dirección de destino del mensaje EAPOL-Start para ser la dirección MAC de la entidad AE; si el punto de acceso AP no tiene conocimiento de la dirección MAC de la entidad AE en este momento operativo, el punto de acceso AP puede establecer la dirección de destino del mensaje EAPOL-Start para ser una dirección de multidifusión de una PAE, en donde el mensaje EAPOL-Start cuya dirección de destino es la dirección de multidifusión de la PAE puede detectarse también y recibirse por la entidad AE.

602. La entidad AE recibe el mensaje EAPOL-Start desde el punto de acceso AP, y reenvía un mensaje de demanda de EAP para demandar la identidad de un equipo UE-1, en donde una dirección origen del mensaje de demanda de EAP es la dirección MAC de la entidad AE y su dirección de destino es una dirección MAC del equipo UE-1.

603. El punto de acceso AP recibe el mensaje de demanda de EAP procedente de la entidad AE, y reenvía el mensaje de demanda de EAP al equipo UE-1.

604. El equipo UE-1 recibe el mensaje de demanda de EAP y tiene conocimiento de que un lado de la red demanda un reconocimiento de identidad y a continuación, el equipo UE-1 envía un mensaje de respuesta de EAP a la entidad AE por intermedio del punto de acceso AP, en donde información tal como el identificador ID se incluye en el mensaje de respuesta.

Puesto que el punto de acceso AP modificó la dirección origen del mensaje de demanda de EAP procedente de la entidad AE, el equipo UE-1 puede tener conocimiento de la dirección MAC de la entidad AE y posteriormente, el equipo UE-1 puede comunicarse con la entidad AE sobre otros mensajes de autenticación EAP utilizando la dirección MAC aprendida de la entidad AE para completar la autenticación de acceso.

605. La entidad AE recibe el mensaje de respuesta de EAP reenviado por el punto de acceso AP y envía un mensaje EAP over Radius a un AS, en donde el mensaje de respuesta de EAP y el identificador ID de identidad del equipo UE-1 se incluyen en el mensaje EAP over Radius.

606. El AS identifica el equipo UE-1 y envía un mensaje de demanda de EAP (TLS Start) a la entidad AE, lo que indica que un algoritmo de autenticación de EAP es EAP-TLS, para iniciar la autenticación EAP. Si el AS selecciona otro algoritmo de autenticación, el mensaje de demanda de EAP (TLS Start) puede indicar, consecuentemente, un algoritmo correspondiente.

607. La entidad AE transmite el mensaje TLS Start al equipo UE-1 por intermedio del punto de acceso AP.

608. El equipo UE-1 envía un mensaje TLS client_hello a la entidad AE por intermedio del punto de acceso AP para dar respuesta al mensaje TLS Start.

609. La entidad AE transmite el mensaje TLS client_hello al AS.

610. El AS envía un mensaje TLS server_hello a la entidad AE, en donde el mensaje puede incluir un certificado de AS, información de intercambio de claves y un conjunto de encriptación de seguridad soportado por el AS y demanda un certificado del equipo UE-1.

611. La entidad AE transmite el mensaje TLS server_hello al equipo UE-1 por intermedio del punto de acceso AP.

612. El equipo UE-1 verifica el certificado de AS y envía un mensaje que incluye un resultado de autenticación, un certificado del equipo UE-1, información de intercambio de claves y un conjunto de encriptación de seguridad soportado por el equipo UE-1 a la entidad AE por intermedio del punto de acceso AP.

613. La entidad AE transmite el mensaje al AS.

614. Después de un resultado satisfactorio de la autenticación, el AS envía un mensaje que incluye un conjunto de encriptación de seguridad seleccionado por el AS para la entidad AE.

615. La entidad AE transmite el mensaje al equipo UE-1 por intermedio del punto de acceso AP.

616. El equipo UE-1 envía un mensaje de respuesta de EAP a la entidad AE por intermedio del punto de acceso AP.

617. La entidad AE transmite el mensaje de respuesta de EAP al AS.

618. El AS envía un mensaje EAP-Success a la entidad AE, indicando que la autenticación es operativamente satisfactoria.

619. La entidad AE transmite el mensaje EAP-Success al equipo UE-1 por intermedio del punto de acceso AP, de modo que el equipo UE-1 tenga conocimiento de que la autenticación es operativamente satisfactoria.

Conviene señalar que en la etapa 603, si después de recibir el mensaje de demanda de EAP procedente de la entidad AE, el punto de acceso AP modifica la dirección origen (la dirección MAC de la entidad AE) para ser una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso AP, el equipo UE-1 puede considerar todavía al punto de acceso AP como una entidad AE para continuar el proceso de autenticación y posteriormente, el punto de acceso AP procesa todavía un mensaje EAP-Start comunicado entre el equipo UE-1 y la entidad AE en conformidad con el método descrito en la forma de realización 3. Por supuesto, el mensaje EAP over RADIUS comunicado entre la entidad AE y el AS no necesita modificarse.

Conviene señalar que la forma de realización se describe tomando a modo de ejemplo, principalmente, un proceso de realización de autenticación de acceso para el equipo UE-1 sobre la base de un algoritmo de autenticación de EAP-TLS. Por supuesto, un algoritmo de autenticación tal como EAP-PEAP o EAP-SIM/AKA puede seleccionarse también para realizar una autenticación de acceso para el equipo UE-1, en donde un proceso de aplicación es el mismo y por ello no se repiten aquí sus detalles.

En conformidad con la descripción que antecede, en la forma de realización, un punto de acceso AP en un desarrollo de autenticación centralizada genera y envía un mensaje de inicio de autenticación EAP cuya dirección origen es una dirección MAC de un equipo UE y cuya dirección de destino es una dirección MAC de una entidad AE, para actuar como un dispositivo proxy para el equipo UE para iniciar un proceso de autenticación de acceso, de modo que el mensaje de inicio de autenticación EAP puede alcanzar la entidad AE, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y realizar la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite a un equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo UE y que está basado en el mecanismo de protocolo IEEE 802.1X.

Con el fin de una mejor puesta en práctica del método anterior en conformidad con las formas de realización de la presente invención, dichas formas de realización dan a conocer, además, un aparato y sistema pertinentes para poner en práctica el método anterior.

Según se ilustra en la Figura 7, un dispositivo de punto de acceso 700 en conformidad con una forma de realización de la presente invención puede incluir un primer módulo de recepción 710, un primer módulo de modificación de dirección 720 y un primer módulo de reenvío 730,

en donde el primer módulo de recepción 710 está configurado para recibir un mensaje de inicio de autenticación EAP enviado por un equipo UE, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección MAC correspondiente a una interfaz de aire del dispositivo de punto de acceso 700 y su dirección origen es una dirección MAC del equipo UE;

el primer módulo de modificación de dirección 720 está configurado para modificar la dirección de destino del mensaje de inicio de autenticación EAP recibido por el primer módulo de recepción 710 para ser una dirección de multidifusión de una PAE o una dirección MAC de una entidad AE; y

el primer módulo de reenvío 730 está configurado para reenviar el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada por el primer módulo de modificación de dirección 720, de modo que la entidad AE inicie la autenticación de acceso para el equipo UE en conformidad con el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada.

En un escenario operativo de aplicación, el dispositivo del punto de acceso AP 700 puede incluir, además, un segundo módulo de recepción, un segundo módulo de modificación de dirección y un segundo módulo de reenvío (no ilustrado en la Figura 7), en donde

el segundo módulo de recepción está configurado para recibir un mensaje de autenticación EAP enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE, y su dirección de destino es la dirección MAC del equipo UE;

el segundo módulo de modificación de dirección está configurado para modificar la dirección origen del mensaje de autenticación EAP recibido por el segundo módulo de recepción para ser la dirección MAC correspondiente a la interfaz de aire del dispositivo de punto de acceso 700, y

el segundo módulo de reenvío está configurado para reenviar el mensaje de autenticación EAP cuya dirección origen es modificada por el segundo módulo de modificación de dirección al equipo UE.

En un escenario operativo de aplicación, el primer módulo de recepción 710 está configurado, además, para recibir un segundo mensaje de autenticación EAP enviado por el equipo UE, en donde el segundo mensaje de autenticación EAP es un mensaje de autenticación enviado por el equipo UE, con la excepción del mensaje de inicio de autenticación EAP, una dirección de destino del segundo mensaje de autenticación EAP es la dirección MAC correspondiente a la interfaz de aire del dispositivo de punto de acceso 700 y su dirección origen es la dirección MAC del equipo UE.

El primer módulo de modificación de dirección 720 está configurado, además, para modificar la dirección de destino del segundo mensaje de autenticación EAP recibido por el primer módulo de recepción para ser la dirección MAC de la entidad AE.

El primer módulo de reenvío 730 está configurado, además, para reenviar el segundo mensaje de autenticación EAP cuya dirección de destino es modificada por el primer módulo de modificación de dirección.

En un escenario operativo de aplicación, el dispositivo de punto de acceso 700 puede incluir, además, un tercer módulo de recepción y un tercer módulo de reenvío (no ilustrado en la Figura 7),

en donde el tercer módulo de recepción está configurado para recibir un tercer mensaje de autenticación EAP

enviado por la entidad AE, en donde una dirección origen del tercer mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo de usuario UE; y

el tercer módulo de reenvío está configurado para reenviar, al equipo UE, el tercer mensaje de autenticación EAP recibido por el tercer módulo de recepción, de modo que el equipo UE tenga conocimiento de la dirección MAC de la entidad AE a partir del tercer mensaje de autenticación EAP.

Conviene señalar que el dispositivo de punto de acceso 700 en la forma de realización puede ser el dispositivo de punto de acceso en la forma de realización 1 o forma de realización 3 del método anterior, y se puede utilizar para servir de ayuda en la puesta en práctica de todas soluciones técnicas en la forma de realización 1 o forma de realización 3 del método anterior, cuyas funciones de módulos funcionales pueden realizarse concretamente en conformidad con el método descrito en las formas de realización del método anterior y puede hacerse referencia a la descripción pertinente en las formas de realización anteriores para sus procesos de puesta en práctica específicos y por ello aquí no se repiten sus detalles.

En conformidad con la descripción que antecede, después del punto de acceso 700 en un desarrollo de autenticación centralizada en conformidad con la forma de realización reciba, desde un equipo UE, un mensaje de inicio de autenticación EAP cuya dirección de destino es una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso 700, el punto de acceso 700 modifica la dirección de destino del mensaje para ser una dirección MAC de una entidad AE, y reenvía el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar la entidad AE en lugar de detenerse en el punto de acceso 700, con el fin de iniciar un proceso de autenticación del acceso para el equipo UE y realizar una autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite al equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo UE y que está basado en el mecanismo del protocolo IEEE 802.1X.

Según se ilustra en la Figura 8, un dispositivo de punto de acceso 800 en conformidad con una forma de realización de la presente invención, puede incluir:

un módulo de generación 810, configurado para generar un mensaje de inicio de autenticación EAP, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección de multidifusión de una PAE o una dirección MAC de una entidad AE, y su dirección origen es una dirección MAC de un equipo de usuario UE;

un módulo de envío 820, configurado para enviar el mensaje de inicio de autenticación EAP generado por el módulo de generación 810;

un módulo de recepción 830, configurado para recibir un mensaje de autenticación EAP enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE, y su dirección de destino es la dirección MAC del equipo de usuario UE; y

un módulo de reenvío 840, configurado para reenviar el mensaje de autenticación EAP recibido por el módulo de recepción 830 al equipo UE, de modo que el equipo UE tenga conocimiento de la dirección MAC de la entidad AE a partir del mensaje de autenticación EAP.

En un escenario operativo de aplicación, con posterioridad, si el punto de acceso 800 recibe, además, un mensaje de autenticación EAP (tal como un mensaje de demanda de EAP para demandar la identidad de un equipo UE u otro mensaje) enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE, el punto de acceso 800 no puede modificar la dirección origen o la dirección de destino del mensaje de autenticación EAP procedente de la entidad AE, pero realiza un reenvío directo del mensaje de autenticación EAP al equipo de usuario UE, de modo que el equipo UE tenga conocimiento de la dirección MAC de la entidad AE a partir del mensaje de autenticación EAP. En este escenario operativo, después de recibir el mensaje de autenticación EAP, el equipo UE puede tener conocimiento de la dirección MAC de una entidad AE real, y puede comunicarse con la entidad AE sobre otros mensajes de autenticación EAP utilizando la dirección MAC aprendida de la entidad AE con posterioridad, con lo que se completa la autenticación de acceso. Dicho de otro modo, después de que el punto de acceso 800 actúe como un dispositivo proxy para el equipo UE para generar y enviar el mensaje de inicio de autenticación EAP (en donde la dirección de destino es la dirección de multidifusión de la PAE o la dirección MAC de la entidad AE, y la dirección origen es la dirección MAC del equipo UE), para iniciar la autenticación de acceso para el equipo UE, el punto de acceso 800 no puede modificar una dirección origen o una dirección de destino de un mensaje de inicio de autenticación EAP comunicado posteriormente entre el equipo UE y la entidad AE; y el equipo UE puede tener conocimiento de la dirección MAC de la entidad AE en función de una respuesta de la entidad AE al mensaje de inicio de autenticación EAP. Por lo tanto, el equipo UE puede enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

Conviene señalar que el dispositivo de punto de acceso 800 en la forma de realización, puede ser el dispositivo de punto de acceso en la forma de realización 2 o forma de realización 4 del método anterior puede utilizarse para servir de ayuda en la puesta en práctica de todas las funciones técnicas en la forma de realización 2 o forma de realización 4 del método anterior, siendo las funciones de sus módulos funcionales puestas en práctica concretamente en conformidad con el método en las formas de realización del método anteriores y puede hacerse referencia a la descripción pertinente en las formas de realización anteriores para sus procesos de puesta en práctica específicos y por ello no se repiten aquí sus detalles.

En conformidad con la descripción que antecede, en la forma de realización, un punto de acceso 800 en el desarrollo de autenticación centralizada genera y envía un mensaje de inicio de autenticación EAP cuya dirección origen es una dirección MAC de un equipo UE y cuya dirección de destino es una dirección MAC de una entidad AE, para actuar como un dispositivo proxy para el equipo UE para iniciar un proceso de autenticación de acceso, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar la entidad AE, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y poner en práctica la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite a un equipo de usuario UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo UE y que está basado en el mecanismo del protocolo IEEE 802.1X.

Según se ilustra en la Figura 9, un dispositivo de punto de acceso 900 en conformidad con una forma de realización de la presente invención puede incluir:

un módulo de generación 910, configurado para generar un mensaje de inicio de autenticación EAP, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección de multidifusión de una PAE o una dirección MAC de una entidad AE y su dirección origen es una dirección MAC de un equipo UE;

un módulo de envío 920, configurado para enviar el mensaje de inicio de autenticación EAP generado por el módulo de generación 910;

un módulo de recepción 930, configurado para recibir un mensaje de autenticación EAP enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE; y

un módulo de modificación y de reenvío 940, configurado para modificar la dirección origen del mensaje de autenticación EAP recibido por el módulo de recepción 930 para ser una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso 900 y para reenviar el mensaje de autenticación EAP con la dirección origen modificada al equipo UE.

En un escenario operativo de aplicación, si el punto de acceso 900 recibe un mensaje de autenticación EAP (a modo de ejemplo, el mensaje de autenticación EAP es un mensaje de demanda de EAP (mensaje EAP-Request) para demandar la identidad de un equipo UE u otro mensaje) enviado por la entidad AE, en donde una dirección origen del mensaje de autenticación EAP es una dirección MAC de la entidad AE, su dirección de destino es una dirección MAC de un equipo UE, el punto de acceso 900 puede modificar la dirección origen del mensaje de autenticación EAP para ser una dirección MAC del punto de acceso 900 y para reenviar el mensaje de autenticación EAP con la dirección origen modificada al equipo UE. En este caso, puesto que la dirección origen del mensaje de autenticación EAP que se reenvía por el punto de acceso 900 y se recibe por el equipo UE es la dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso 900, el equipo UE puede todavía utilizar el punto de acceso 900 como una entidad AE para continuar la autenticación EAP. Posteriormente, si el punto de acceso 900 recibe, además, otro mensaje de autenticación EAP enviado por el equipo UE, en donde el mensaje de autenticación EAP es un mensaje de autenticación (a modo de ejemplo, un mensaje de respuesta de EAP que incluye una identidad de UE (ID) u otro mensaje de autenticación EAP) enviado por el equipo UE, con la excepción del mensaje de inicio de autenticación EAP, una dirección de destino del mensaje de autenticación EAP es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso 900 y su dirección origen es la dirección MAC del equipo UE, el punto de acceso 900 puede modificar la dirección de destino del mensaje de autenticación EAP para ser la dirección MAC de la entidad AE y reenviar el mensaje de autenticación EAP cuya dirección de destino es modificada. Dicho de otro modo, el punto de acceso AP puede modificar direcciones origen o direcciones de destino de todos los mensajes de autenticación EAP comunicados entre el equipo UE y la entidad AE, modificar la dirección de destino del mensaje de autenticación EAP procedente del equipo UE para ser la dirección MAC de la entidad AE y modificar la dirección origen del mensaje de autenticación EAP procedente de la entidad AE para ser la dirección MAC del punto de acceso 900; y el equipo UE puede considerar siempre el punto de acceso 900 como una entidad AE para la autenticación EAP. Por lo tanto, el equipo UE puede enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

Conviene señalar que el dispositivo de punto de acceso 900 en la forma de realización puede ser un dispositivo de punto de acceso en la forma de realización 2 o forma de realización 4 del método anterior, y puede utilizarse para

servir de ayuda en la puesta en práctica de todas las soluciones técnicas en la forma de realización 2 o forma de realización 4 del método anterior, siendo las funciones de sus módulos funcionales puestas en práctica concretamente en conformidad con el método en las formas de realización del método anterior y puede hacerse referencia a la descripción pertinente en las formas de realización anteriores para sus procesos de puesta en práctica específicos y por ello no se repiten aquí sus detalles.

En conformidad con la descripción que antecede, en la forma de realización, un punto de acceso 900 en el desarrollo de autenticación centralizada genera y envía un mensaje de inicio de autenticación EAP cuya dirección origen es una dirección MAC de un equipo UE y cuya dirección de destino es una dirección MAC de una entidad AE, para actuar como un dispositivo proxy para el equipo UE para iniciar un proceso de autenticación de acceso, de modo que el mensaje de inicio de autenticación EAP puede alcanzar la entidad AE, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y poner en práctica la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite a un equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo UE y sobre la base del mecanismo del protocolo IEEE 802.1X.

Según se ilustra en la Figura 10, una forma de realización de la presente invención da a conocer un sistema para la autenticación centralizada 802.1X en una red de área local inalámbrica, en donde una red de área local inalámbrica incluye una entidad de autenticación 1010, un punto de acceso 1020 y al menos un equipo de usuario 1030 y la entidad de autenticación 1010 está conectada a al menos un equipo de usuario 1030 por intermedio del punto de acceso 1020,

en donde el punto de acceso 1020 está configurado para recibir un mensaje de inicio de autenticación EAP del protocolo de autenticación extensiva enviado por el equipo de usuario 1030, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección MAC de control de acceso al medio del punto de acceso 1020, y su dirección origen es una dirección MAC del equipo de usuario 1030; modificar la dirección de destino del mensaje de inicio de autenticación EAP para ser una dirección de multidifusión de una entidad de acceso de puerto o una dirección MAC de la entidad de autenticación 1010; y reenviar el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada, de modo que la entidad de autenticación 1010 inicie la autenticación de acceso para el equipo de usuario 1030, en conformidad con el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada.

En un escenario operativo de aplicación, si el punto de acceso 1020 recibe, además, un mensaje de autenticación EAP (tal como un mensaje de demanda de EAP para demandar la identidad del equipo de usuario 1030 u otro mensaje) enviado por la entidad de autenticación 1010, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad de autenticación 1010, y su dirección de destino es la dirección MAC del equipo de usuario 1030, el punto de acceso puede modificar la dirección origen del mensaje de autenticación EAP para ser la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso y reenviar el mensaje de autenticación EAP con la dirección origen modificada al equipo de usuario 1030. En este caso, puesto que la dirección origen del mensaje de autenticación EAP que se reenvía por el punto de acceso 1020 y se recibe por el equipo de usuario 1030 es la dirección MAC del punto de acceso 1020, el equipo de usuario 1030 puede considerar todavía el punto de acceso 1020 como una entidad AE para continuar la autenticación EAP. Si el punto de acceso 1020 recibe, además, un segundo mensaje de autenticación EAP enviado por el equipo de usuario 1030, en donde el segundo mensaje de autenticación EAP es un mensaje de autenticación enviado por el equipo de usuario 1030 con la excepción del mensaje de inicio de autenticación EAP (el segundo mensaje de autenticación EAP es, a modo de ejemplo, un mensaje de respuesta de EAP que incluye la identidad (ID) del equipo de usuario 1030 u otro mensaje de autenticación EAP), una dirección de destino del segundo mensaje de autenticación EAP es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso 1020 y su dirección origen es la dirección MAC del equipo de usuario 1030, el punto de acceso 1020 puede modificar la dirección de destino del segundo mensaje de autenticación EAP para ser la dirección MAC de la entidad de autenticación 1010 y reenviar el segundo mensaje de autenticación EAP cuya dirección de destino es modificada. Dicho de otro modo, el punto de acceso 1020 puede modificar las direcciones origen o las direcciones de destino de todos los mensajes de autenticación EAP comunicados entre el equipo de usuario 1030 y la entidad de autenticación 1010, modificar una dirección de destino de un mensaje de autenticación EAP desde el equipo de usuario 1030 a la dirección MAC de la entidad de autenticación 1010 y modificar una dirección origen de un mensaje de autenticación EAP desde la entidad de autenticación 1010 para ser la dirección MAC del punto de acceso 1020; y el equipo de usuario 1030 puede considerar siempre al punto de acceso 1020 como una entidad AE para la autenticación EAP. Puesto que el equipo de usuario 1030 tiene conocimiento de la dirección MAC del punto de acceso 1020 antes de la autenticación, el equipo de usuario 1030 puede enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

En otro escenario operativo de aplicación, si el punto de acceso 1020 recibe, además, un tercer mensaje de autenticación EAP (tal como un mensaje EAP-Request para demandar la identidad del equipo de usuario 1030 u otro mensaje) enviado por la entidad de autenticación 1010, en donde una dirección origen del tercer mensaje de autenticación EAP es la dirección MAC de la entidad de autenticación 1010, y su dirección de destino es la dirección

MAC del equipo de usuario 1030, el punto de acceso 1020 no puede modificar la dirección origen o la dirección de destino del tercer mensaje de autenticación EAP, pero puede reenviar directamente el tercer mensaje de autenticación EAP al equipo de usuario 1030, de modo que el equipo de usuario 1030 pueda tener conocimiento de la dirección MAC de la entidad de autenticación 1010 a partir del tercer mensaje de autenticación EAP. En este escenario operativo, después de recibir el tercer mensaje de autenticación EAP, el equipo de usuario 1030 puede tener conocimiento de la dirección MAC de una entidad de autenticación real, y puede comunicarse con la entidad de autenticación 1010 sobre otros mensajes de autenticación EAP utilizando la dirección MAC aprendida de la entidad de autenticación 1010 con posterioridad, con lo que se completa la autenticación de acceso. Dicho de otro modo, el punto de acceso 1020 solamente puede modificar la dirección de destino del mensaje de inicio de autenticación EAP (un primer mensaje de autenticación EAP procedente del equipo de usuario 1030), pero no puede modificar la dirección origen o la dirección de destino de un mensaje de inicio de autenticación EAP comunicado posteriormente entre el equipo de usuario 1030 y la entidad de autenticación 1010; y el equipo de usuario 1030 puede tener conocimiento de la dirección MAC de la entidad de autenticación 1010 en conformidad con una respuesta de la entidad de autenticación 1010 al mensaje de inicio de autenticación EAP; de modo que el equipo de usuario 1030 pueda enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

En un escenario operativo de aplicación, el punto de acceso 1020 puede configurarse, además, para generar un mensaje de inicio de autenticación EAP, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección de multidifusión de una entidad de acceso de puerto o una dirección MAC de la entidad de autenticación 1010 y su dirección origen es una dirección MAC de un segundo equipo de usuario (no ilustrado en la Figura 10); enviar el mensaje de inicio de autenticación EAP; recibir un mensaje de autenticación EAP enviado por la entidad de autenticación 1010, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad de autenticación 1010 y su dirección de destino es la dirección MAC del segundo equipo de usuario; y modificar la dirección origen del mensaje de autenticación EAP para ser una dirección MAC correspondiente a una interfaz de aire del punto de acceso 1020 y reenviar el mensaje de autenticación EAP con la dirección origen modificada al segundo equipo de usuario.

Conviene señalar que el punto de acceso 1020 en la forma de realización, puede ser el dispositivo de punto de acceso en la forma de realización 1 o forma de realización 3 del método anterior, y puede utilizarse para servir de ayuda en la puesta en práctica de todas las soluciones técnicas en la forma de realización 1 o forma de realización 3 del método anterior, cuyas funciones de los módulos funcionales pueden ponerse en práctica concretamente en conformidad con el método en las formas de realización del método anteriores y puede hacerse referencia a la descripción pertinente en las formas de realización anteriores para sus procesos de puesta en práctica específicos y por ello no se repiten aquí de nuevo sus detalles.

Según se ilustra en la Figura 11, una forma de realización de la presente invención da a conocer un sistema para la autenticación centralizada 802.1X en una red de área local inalámbrica, en donde una red de área local inalámbrica incluye una entidad de autenticación 1110, un punto de acceso 1120 y al menos un equipo de usuario 1130 y la entidad de autenticación 1110 está conectada a al menos un equipo de usuario 1130 por intermedio del punto de acceso 1120,

en donde el punto de acceso 1120 está configurado para generar un mensaje de inicio de autenticación EAP, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección de multidifusión de una entidad de acceso de puerto o una dirección MAC de la entidad de autenticación 1110 y su dirección origen es una dirección MAC del equipo UE; enviar el mensaje de inicio de autenticación EAP; recibir un mensaje de autenticación EAP enviado por la entidad de autenticación 1110, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad de autenticación 1110 y su dirección de destino es la dirección MAC del equipo de usuario 1130; y reenviar el mensaje de autenticación EAP al equipo de usuario 1130, de modo que el equipo de usuario 1130 tenga conocimiento de la dirección MAC de la entidad de autenticación a partir del mensaje de autenticación EAP o modificar la dirección origen del mensaje de autenticación EAP para ser una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso 1120 y reenviar el mensaje de autenticación EAP con la dirección origen modificada al equipo de usuario 1130.

En un escenario operativo de aplicación, si el punto de acceso 1120 recibe un mensaje de autenticación EAP (tal como un mensaje de demanda de EAP (mensaje EAP-Request) para demandar la identidad del equipo de usuario 1130 u otro mensaje) enviado por la entidad de autenticación 1110, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de una entidad AE, y su dirección de destino es la dirección MAC del equipo de usuario 1130, el punto de acceso 1120 puede modificar la dirección origen del mensaje de autenticación EAP para ser la dirección MAC del punto de acceso 1120 y reenviar el mensaje de autenticación EAP con la dirección de origen modificada al equipo de usuario 1130. En este caso, puesto que la dirección origen del mensaje de autenticación EAP que se reenvía por el punto de acceso 1120 y se recibe por el equipo de usuario 1130 es la dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso, el equipo de usuario 1130 puede considerar todavía al punto de acceso 1120 como una entidad AE para continuar la autenticación EAP. Posteriormente, si el punto de acceso 1120 recibe, además, otro mensaje de autenticación EAP enviado por equipo UE, en donde el mensaje de autenticación EAP es un mensaje de autenticación (a modo de

ejemplo, un mensaje EAP-Response que incluye la identidad (ID) del equipo de usuario 1130 u otro mensaje de autenticación EAP) enviado por el equipo de usuario 1130, con la excepción del mensaje de inicio de autenticación EAP, una dirección de destino del mensaje de autenticación EAP es la dirección MAC (tal como un identificador BSSID) correspondiente a la interfaz de aire del punto de acceso, y su dirección origen es la dirección MAC del equipo de usuario 1130, el punto de acceso 1120 puede modificar la dirección de destino del mensaje de autenticación EAP para ser la dirección MAC de la entidad de autenticación 1110, y reenviar el mensaje de autenticación EAP cuya dirección de destino es modificada. Dicho de otro modo, el punto de acceso 1120 puede modificar las direcciones origen y direcciones de destino de todos los mensajes de autenticación EAP comunicados entre el equipo de usuario 1130 y la entidad de autenticación 1110, modificar una dirección de destino de un mensaje de autenticación EAP procedente del equipo de usuario 1130 a la dirección MAC de la entidad de autenticación 1110 y modificar una dirección origen de un mensaje de autenticación EAP procedente de la entidad de autenticación 1110 para ser la dirección MAC del punto de acceso 1120; y el equipo UE puede considerar siempre al punto de acceso 1120 como una entidad AE para la autenticación EAP. Por lo tanto, el equipo de usuario 1130 puede enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

En otro escenario operativo de aplicación, posteriormente, si el punto de acceso 1120 recibe, además, un mensaje de autenticación EAP (tal como un mensaje EAP-Request para demandar la identidad del equipo de usuario 1130 u otro mensaje) enviado por la entidad de autenticación 1110, en donde una dirección origen del mensaje de autenticación EAP es la dirección MAC de la entidad de autenticación 1110, y su dirección de destino es la dirección MAC del equipo de usuario 1130, el punto de acceso 1120 no puede modificar la dirección origen o la dirección de destino del mensaje de autenticación EAP procedente de la entidad de autenticación 1110, pero puede reenviar directamente el mensaje de autenticación EAP al equipo de usuario 1130, de modo que el equipo de usuario 1130 tenga conocimiento de la dirección MAC de la entidad de autenticación 1110 a partir del mensaje de autenticación EAP. En este escenario operativo, después de recibir el mensaje de autenticación EAP, el equipo de usuario 1130 puede tener conocimiento de la dirección MAC de una entidad de autenticación real 1110 y puede comunicarse con la entidad de autenticación 1110 sobre otros mensajes de autenticación EAP utilizando la dirección MAC aprendida de la entidad de autenticación 1110 posteriormente, por lo que se completa con la autenticación de acceso. Dicho de otro modo, después de que el punto de acceso 1120 actúe como un dispositivo proxy para el equipo de usuario 1130 para generar y enviar el mensaje de inicio de autenticación EAP (en donde la dirección de destino es una dirección de multidifusión de una entidad de acceso de puerto o la dirección MAC de la entidad de autenticación 1110, y la dirección origen es la dirección MAC del equipo de usuario 1130), para iniciar la autenticación de acceso para el equipo de usuario 1130, el punto de acceso 1120 no puede modificar una dirección origen o la dirección de destino de un mensaje de inicio de autenticación EAP comunicado posteriormente entre el equipo de usuario 1130 y la entidad de autenticación 1110; y el equipo de usuario 1130 puede tener conocimiento de la dirección MAC de la entidad de autenticación 1110 en conformidad con una respuesta de la entidad de autenticación 1110 al mensaje de inicio de autenticación EAP, de modo que el equipo de usuario 1130 pueda enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X.

En un escenario operativo de aplicación, el punto de acceso 1120 está configurado, además para: recibir un mensaje de inicio de autenticación EAP del protocolo de autenticación extensiva enviado por un tercer equipo de usuario, en donde una dirección de destino del mensaje de inicio de autenticación EAP es una dirección MAC de control de acceso al medio correspondiente a una interfaz de aire del punto de acceso 1120 y su dirección origen es una dirección MAC del tercer equipo de usuario; modificar la dirección de destino del mensaje de inicio de autenticación EAP para ser la dirección de multidifusión de la entidad de puerto de acceso o la dirección MAC de la entidad de autenticación 1110; y reenviar el mensaje de inicio de autenticación EAP cuya dirección de destino es modificada, de modo que la entidad de autenticación 1110 inicie la autenticación de acceso para el tercer equipo de usuario en conformidad con el mensaje de inicio de autenticación EAP cuya dirección de destino se modifica.

Conviene señalar que el punto de acceso 1120, en la forma de realización puede ser el dispositivo de punto de acceso en la forma de realización 2 o forma de realización 4 del método anterior y puede utilizarse para servir de ayuda en la puesta en práctica de todas las soluciones técnicas en la forma de realización 2 o forma de realización 4 del método anterior, cuyas funciones de los módulos funcionales pueden ponerse en práctica concretamente en conformidad con el método en las formas de realización del método anteriores, y puede hacerse referencia a la descripción pertinente en las formas de realización anteriores para sus procesos de puesta en práctica específicos y por ello no se repiten aquí sus detalles.

Conviene señalar que, para la finalidad de una breve descripción, cada una de las formas de realización anteriores del método se describe como una combinación de una serie de acciones; sin embargo, los expertos en esta técnica deben entenderse que la presente invención no está limitada por la secuencia de las acciones descritas porque algunas etapas pueden realizarse en otras secuencias o simultáneamente en conformidad con la presente invención. Además, los expertos en esta técnica deben entender, además, que las formas de realización descritas en la especificación son formas de realización preferidas y las acciones y los módulos aquí descritos no se requieren necesariamente para la presente invención.

En las formas de realización anteriores, las formas de realización resaltan aspectos diferentes, y para la parte no

descrita en detalle en una forma de realización, puede hacerse referencia a la descripción pertinente de otras formas de realización.

En conclusión, en una solución técnica según una forma de realización de la presente invención, después de que un punto de acceso AP en el desarrollo de autenticación centralizada reciba, desde un equipo UE, un mensaje de inicio de autenticación EAP cuya dirección de destino es una dirección MAC (tal como un identificador BSSID) correspondiente a una interfaz de aire del punto de acceso AP, el punto de acceso AP modifica la dirección de destino del mensaje para ser una dirección MAC de una entidad AE y reenviar el mensaje de inicio de autenticación EAP cuya dirección de destino se modifica, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar la entidad AE en lugar de detenerse en el punto de acceso AP, con el fin de iniciar un proceso de autenticación de acceso para el equipo UE y para poner en práctica la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite al equipo UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo UE y está basado en el mecanismo del protocolo IEEE 802.1X.

En otra solución técnica dada a conocer por una forma de realización de la presente invención, un punto de acceso AP en el desarrollo de autenticación centralizada genera y envía un mensaje de inicio de autenticación EAP cuya dirección origen es una dirección MAC de un equipo UE y cuya dirección de destino es una dirección MAC de una entidad AE, para actuar como un dispositivo proxy para el equipo de usuario UE para iniciar un proceso de autenticación de acceso, de modo que el mensaje de inicio de autenticación EAP pueda alcanzar una entidad AE, con el fin de iniciar un proceso de autenticación de acceso para el equipo de usuario UE y para poner en práctica la autenticación centralizada 802.1X para el equipo UE en una red de área local inalámbrica. Además, este mecanismo permite a un equipo de usuario UE enviar todos los mensajes de autenticación EAP en el modo de unidifusión en conformidad con la especificación del protocolo IEEE 802.1X; por lo tanto, resulta innecesario modificar un programa de autenticación que se establece en el equipo de usuario UE y está basado en el mecanismo del protocolo IEEE 802.1X.

Los expertos ordinarios en esta técnica pueden entender que la totalidad o una parte de las etapas de los métodos en conformidad con las formas de realización pueden ponerse en práctica mediante un programa informático que proporcione instrucciones a los equipos físicos pertinentes. El programa puede memorizarse en un soporte de memorización legible por ordenador, y el medio de memorización puede incluir una memoria de solamente lectura, una memoria de acceso aleatorio, un disco magnético o un CD-ROM.

Un método, un aparato y un sistema para la autenticación centralizada 802.1X en una red de área local inalámbrica, en conformidad con las formas de realización de la presente invención, se describió en detalle con anterioridad. El principio y las formas de realización de la presente invención se describen utilizando ejemplos concretos en este caso. Las formas de realización anteriores se describen para servir de ayuda para entender el método y la idea básica de la presente invención. Asimismo, los expertos en esta técnica pueden realizar variaciones a las formas de realización específicas y el alcance de aplicación sobre la base de la idea inventiva de la presente invención. Por lo tanto, el contenido de la especificación no deberá interpretarse como una limitación para el alcance de protección de la presente invención.

REIVINDICACIONES

1. Un método para la autenticación centralizada según el protocolo 802.1X en una red de área local inalámbrica, en donde la red de área local inalámbrica comprende una entidad de autenticación, AE, un punto de acceso, AP, y al menos un equipo de usuario, UE, estando la entidad AE conectada a al menos un equipo de usuario UE por intermedio del punto de acceso AP, caracterizado por cuanto que el método comprende:

la generación (410), por el punto de acceso AP, de un mensaje de inicio de autenticación según el protocolo de autenticación extensiva, mensaje EAPOL-Start, después de la asociación de un equipo de usuario UE con el punto de acceso AP; en donde una dirección de destino del mensaje EAPOL-Start es una dirección de multidifusión de una Entidad de Acceso al Puerto, PAE, o de un Control de Acceso al Medio, MAC, de la entidad AE y una dirección origen del mensaje EAPOL-Start es una dirección MAC del equipo de usuario UE asociado;

el envío (420), por el punto de acceso AP, del mensaje EAPOL-Start;

la recepción (430), por el punto de acceso AP, de un primer mensaje de autenticación EAP procedente de la entidad AE; en donde una dirección origen del primer mensaje de autenticación EAP es la dirección MAC de la entidad AE, y una dirección de destino del primer mensaje de autenticación EAP es la dirección MAC del equipo de usuario UE asociado; y

la modificación (440), por el punto de acceso AP, de la dirección origen del primer mensaje de autenticación EAP para ser una dirección MAC correspondiente a una interfaz de aire del punto de acceso AP; y

el reenvío (440), por el punto de acceso AP, del mensaje de autenticación EAP modificado al equipo UE asociado con el fin de que el equipo UE asociado utilice el punto de acceso AP como una entidad AE para continuar la autenticación del protocolo EAP.

2. El método según la reivindicación 1, en donde el método comprende, además:

la recepción de un segundo mensaje de autenticación EAP enviado por el equipo UE asociado, en donde el segundo mensaje de autenticación EAP es un mensaje de autenticación enviado por el equipo de usuario UE asociado, con la excepción del mensaje EAPOL-Start, una dirección de destino del segundo mensaje de autenticación EAP es la dirección MAC correspondiente a la interfaz de aire del punto de acceso AP y su dirección origen es la dirección MAC del equipo de usuario UE asociado;

la modificación de la dirección de destino del segundo mensaje de autenticación EAP para ser la dirección MAC de la entidad AE; y

el reenvío del segundo mensaje de autenticación EAP cuya dirección de destino se modifica.

3. El método según la reivindicación 1, en donde el método comprende, además:

la recepción de un tercer mensaje de autenticación EAP enviado por la entidad AE, en donde una dirección origen del tercer mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo UE asociado; y

el reenvío del tercer mensaje de autenticación EAP al equipo de usuario UE asociado, de modo que el equipo UE asociado tenga conocimiento de la dirección MAC de la entidad AE a partir del tercer mensaje de autenticación EAP.

4. El método según la reivindicación 1, en donde la dirección MAC correspondiente a la interfaz de aire del punto de acceso AP es el identificador BSSID.

5. Un dispositivo de punto de acceso, AP, caracterizado por cuanto que comprende:

un módulo de generación (910), configurado para generar un mensaje de inicio de autenticación de protocolo de autenticación extensiva, mensaje EAPOL-Start, después de que un equipo de usuario UE se asocie con el dispositivo de AP; en donde una dirección de destino del mensaje EAPOL-Start es una dirección de multidifusión de una Entidad de Acceso al Puerto, PAE, o de un Control de Acceso al Medio, MAC, de una entidad de autenticación, AE, y una dirección origen del mensaje EAPOL-Start es una dirección MAC del equipo de usuario UE asociado;

un módulo de envío (920), configurado para enviar el mensaje EAPOL-Start;

un módulo de recepción (930), configurado para recibir un primer mensaje de autenticación EAP procedente de la entidad AE; en donde una dirección origen del primer mensaje de autenticación EAP es la dirección MAC de la entidad AE y una dirección de destino del primer mensaje de autenticación EAP es la dirección MAC del equipo de usuario UE asociado;

un módulo de modificación y reenvío (940), configurado para modificar la dirección origen del primer mensaje de autenticación EAP para ser una dirección MAC correspondiente a una interfaz de aire del punto de acceso AP; y para reenviar el mensaje de autenticación EAP modificado al equipo UE asociado con el fin de que el equipo UE asociado utilice el punto de acceso AP como una entidad AE para continuar la autenticación EAP.

6. El dispositivo AP según la reivindicación 5, en donde el dispositivo AP está configurado, además, para:

recibir un segundo mensaje de autenticación EAP enviado por el equipo UE asociado, en donde el segundo mensaje de autenticación EAP es un mensaje de autenticación enviado por el equipo de usuario UE asociado, con la excepción del mensaje EAPOL-Start, una dirección de destino del segundo mensaje de autenticación EAP es la dirección MAC correspondiente a la interfaz de aire del punto de acceso AP y su dirección origen es la dirección MAC del equipo de usuario UE asociado;

modificar la dirección de destino del segundo mensaje de autenticación EAP para ser la dirección MAC de la entidad AE; y

reenviar el segundo mensaje de autenticación EAP cuya dirección de destino es modificada.

7. El dispositivo de punto de acceso según la reivindicación 5, en donde el dispositivo AP está configurado, además, para:

recibir un tercer mensaje de autenticación EAP enviado por la entidad AE, en donde una dirección origen del tercer mensaje de autenticación EAP es la dirección MAC de la entidad AE y su dirección de destino es la dirección MAC del equipo de usuario UE asociado; y

reenviar el tercer mensaje de autenticación EAP al equipo de usuario UE asociado, de modo que el equipo de usuario UE asociado tenga conocimiento de la dirección MAC de la entidad AE a partir del tercer mensaje de autenticación EAP.

8. Un sistema para autenticación centralizada según el protocolo 802.1X en una red de área local inalámbrica, en donde la red de área local inalámbrica comprende un punto de acceso en conformidad con cualquiera de las reivindicaciones 5 a 7, una entidad de autenticación, AE y al menos un equipo de usuario UE, estando la entidad AE conectada a al menos un equipo de usuario UE por intermedio del punto de acceso.

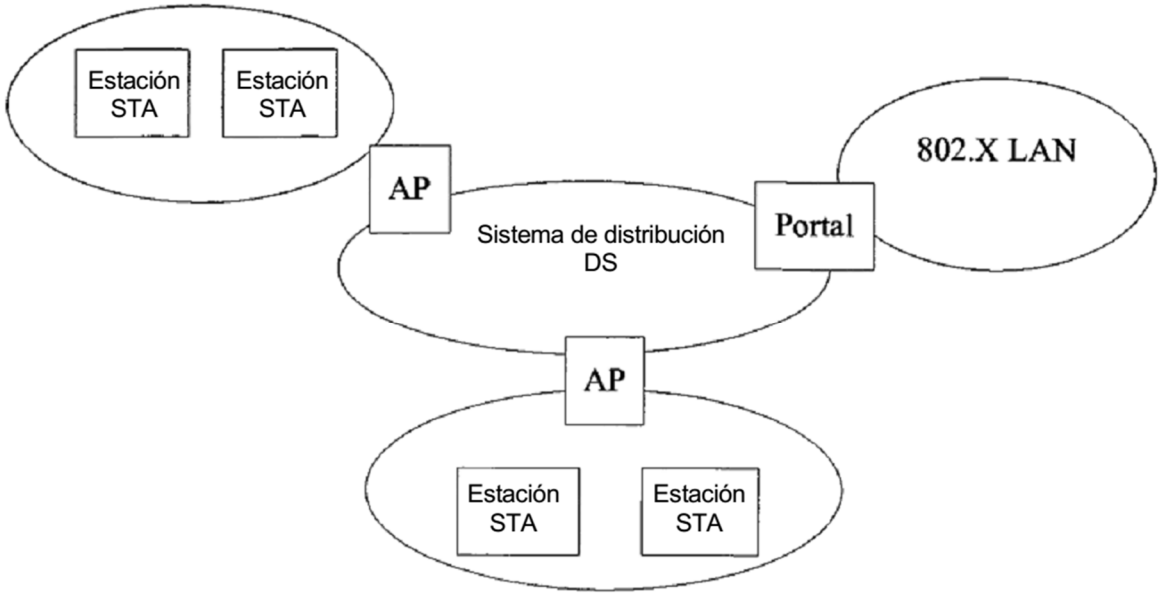
Estación STA
Estación STA
AP
Sistema de distribución DS
Portal
802.X LAN
AP
Estación STA
Estación STA

FIG. 1

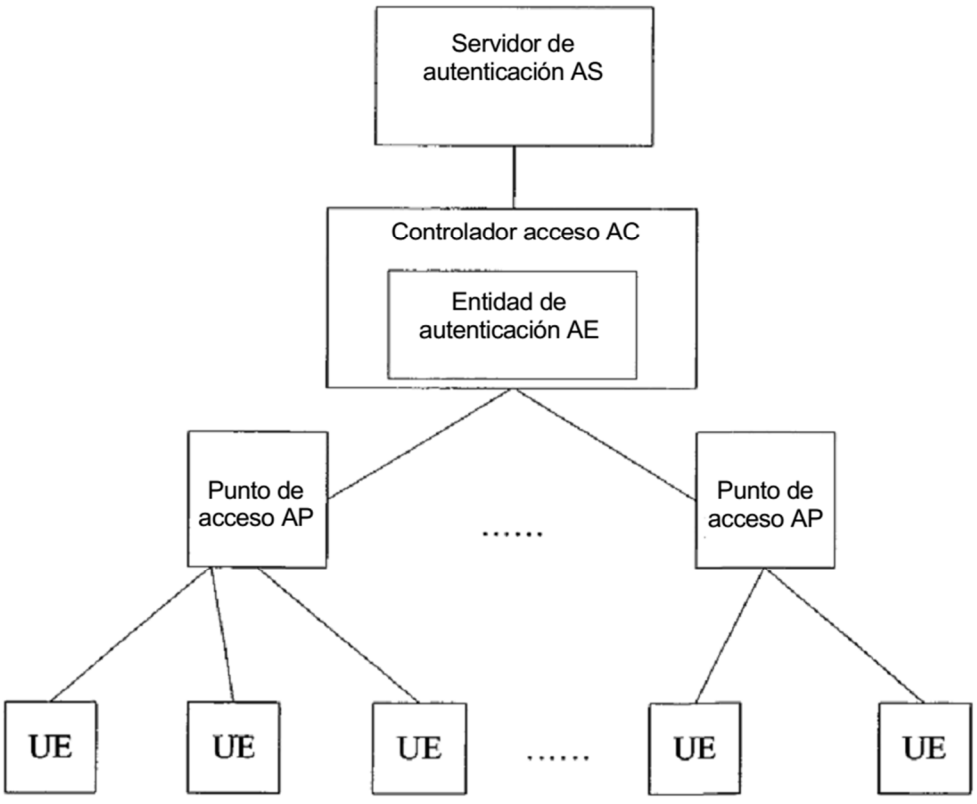
Servidor de autenticación AS
Controlador acceso AC
Entidad de autenticación AE
Punto de acceso AP
.....
Punto de acceso AP
UE
UE
UE
.....
UE
UE

FIG. 2

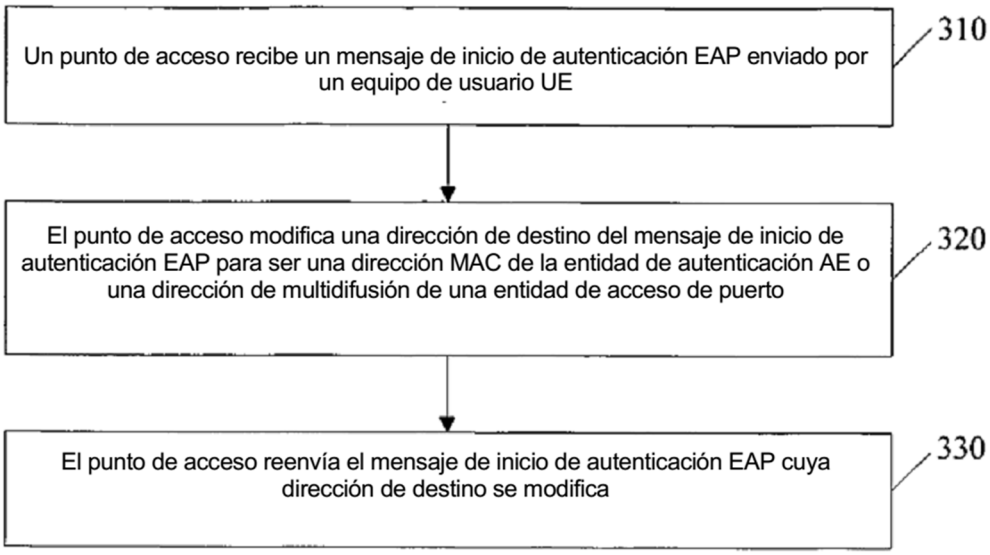
Un punto de acceso recibe un mensaje de inicio de autenticación EAP enviado por un equipo de usuario UE
310
El punto de acceso modifica una dirección de destino del mensaje de inicio de autenticación EAP para ser una dirección MAC de la entidad de autenticación AE o una dirección de multidifusión de una entidad de acceso de puerto
320
El punto de acceso reenvía el mensaje de inicio de autenticación EAP cuya dirección de destino se modifica
330

FIG. 3

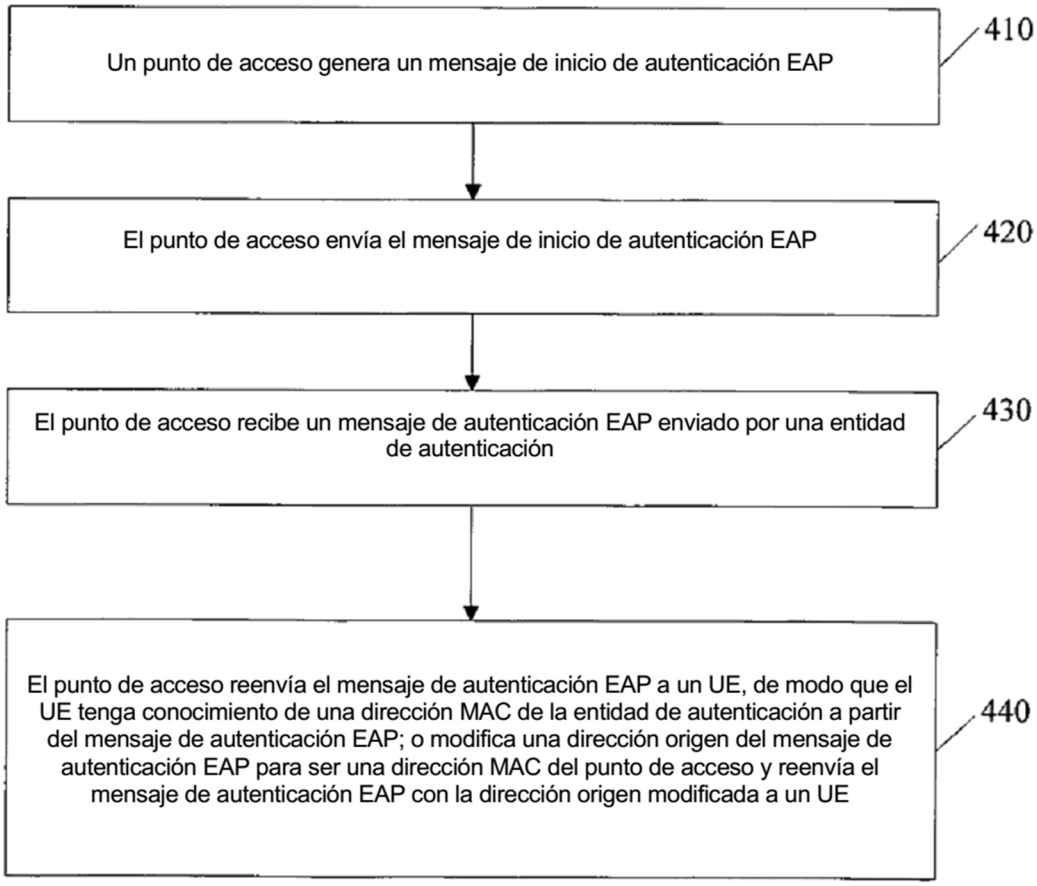
Un punto de acceso genera un mensaje de inicio de autenticación EAP
410
El punto de acceso envía el mensaje de inicio de autenticación EAP
420
El punto de acceso recibe un mensaje de autenticación EAP enviado por una entidad de autenticación
430
El punto de acceso reenvía el mensaje de autenticación EAP a un UE, de modo que el UE tenga conocimiento de una dirección MAC de la entidad de autenticación a partir del mensaje de autenticación EAP; o modifica una dirección origen del mensaje de autenticación EAP para ser una dirección MAC del punto de acceso y reenvía el mensaje de autenticación EAP con la dirección origen modificada a un UE
440

FIG. 4

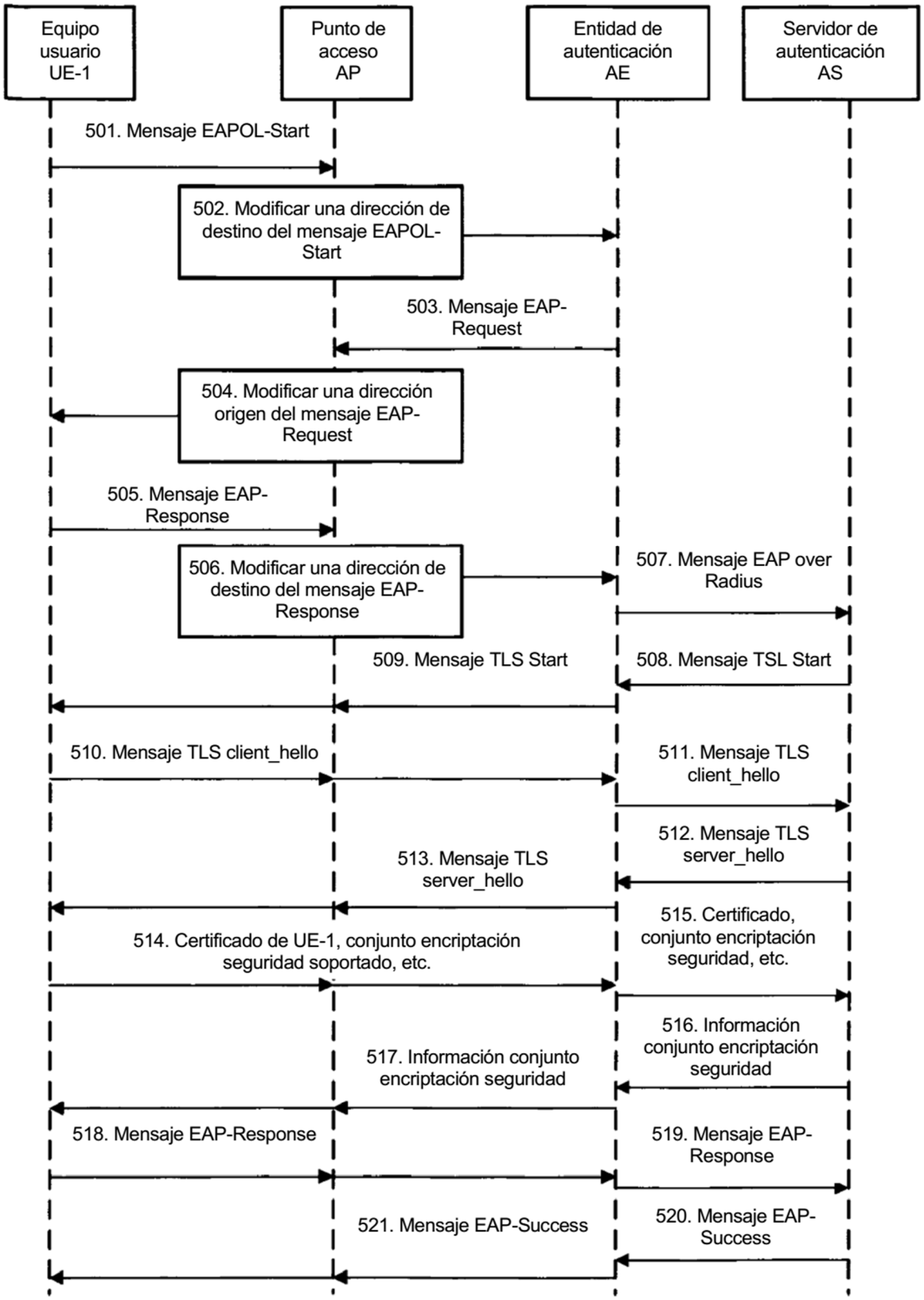
Equipo usuario UE-1
Punto de acceso AP
Entidad de autenticación AE
Servidor de autenticación AS
501. Mensaje EAPOL-Start
502. Modificar una dirección de destino del mensaje EAPOL-Start
503. Mensaje EAP-Request
504. Modificar una dirección origen del mensaje EAP-Request
505. Mensaje EAP-Response
506. Modificar una dirección de destino del mensaje EAP-Response
507. Mensaje EAP over Radius
508. Mensaje TSL Start
509. Mensaje TLS Start
510. Mensaje TLS client_hello
511. Mensaje TLS client_hello
512. Mensaje TLS server_hello
513. Mensaje TLS server_hello
514. Certificado de UE-1, conjunto encriptación seguridad soportado, etc.
515. Certificado, conjunto encriptación seguridad, etc.
516. Información conjunto encriptación seguridad
517. Información conjunto encriptación seguridad
518. Mensaje EAP-Response
519. Mensaje EAP-Response
520. Mensaje EAP-Success
521. Mensaje EAP-Success

FIG. 5

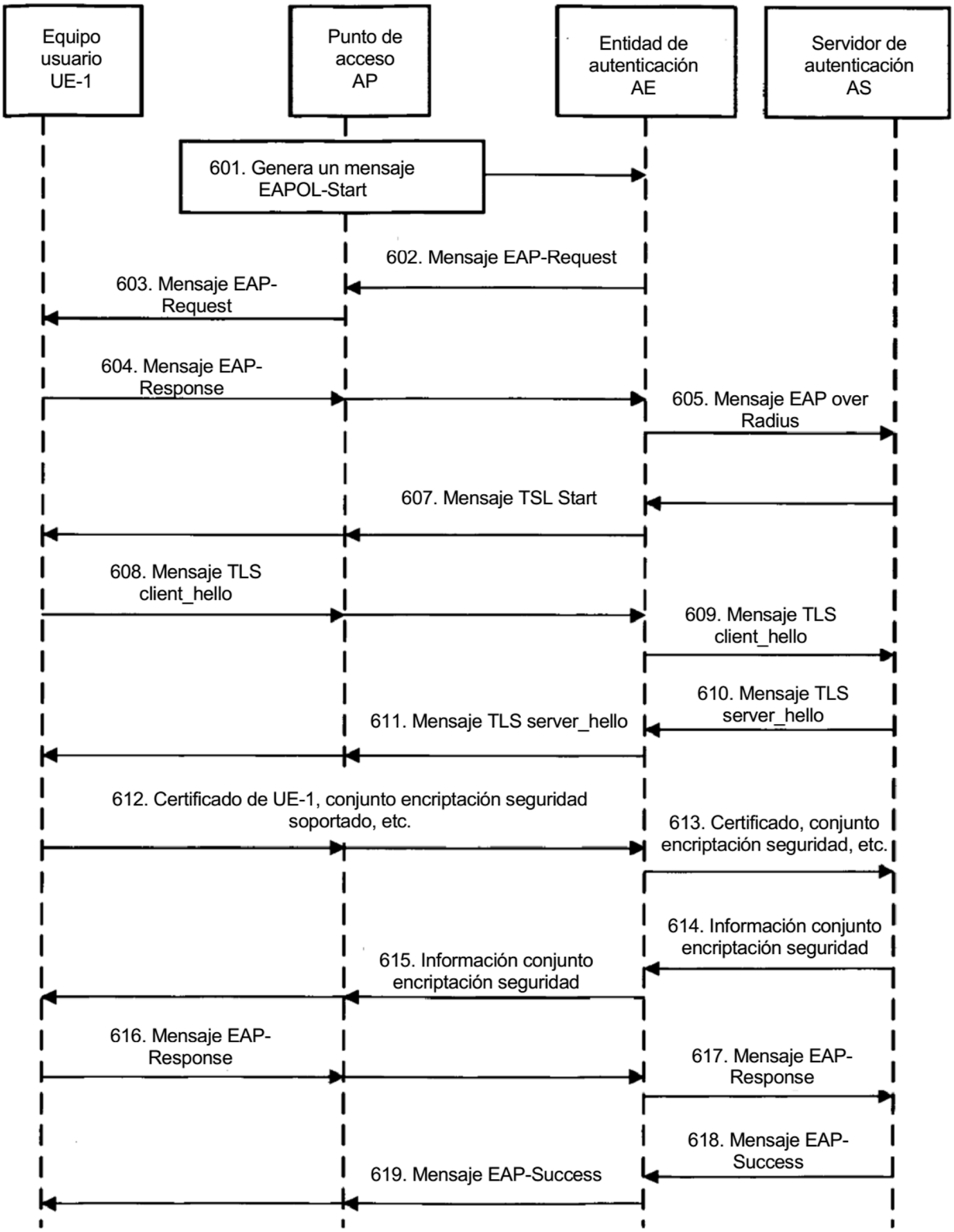
Equipo usuario UE-1
Punto de acceso AP
Entidad de autenticación AE
Servidor de autenticación AS
601. Genera un mensaje EAPOL-Start
602. Mensaje EAP-Request
603. Mensaje EAP-Request
604. Mensaje EAP-Response
605. Mensaje EAP over Radius
607. Mensaje TSL Start
608. Mensaje TLS client_hello
609. Mensaje TLS client_hello
610. Mensaje TLS server_hello
611. Mensaje TLS server_hello
612. Certificado de UE-1, conjunto encriptación seguridad soportado, etc.
613. Certificado, conjunto encriptación seguridad, etc.
614. Información conjunto encriptación seguridad
615. Información conjunto encriptación seguridad
616. Mensaje EAP-Response
617. Mensaje EAP-Response
618. Mensaje EAP-Success
619. Mensaje EAP-Success

FIG. 6

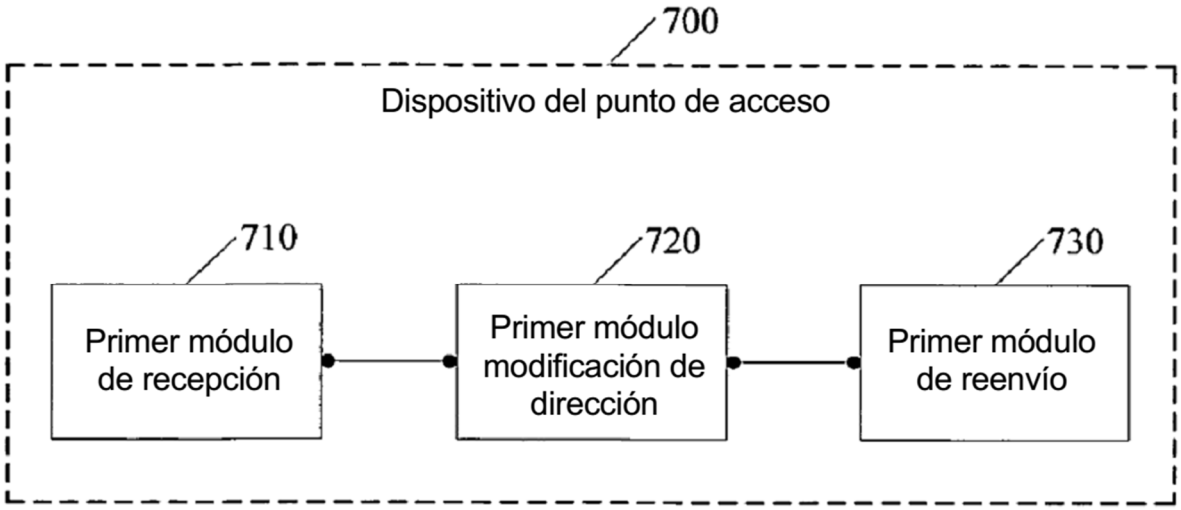
700
Dispositivo del punto de acceso
710
Primer módulo de recepción
720
Primer módulo modificación de dirección
730
Primer módulo de reenvío

FIG. 7

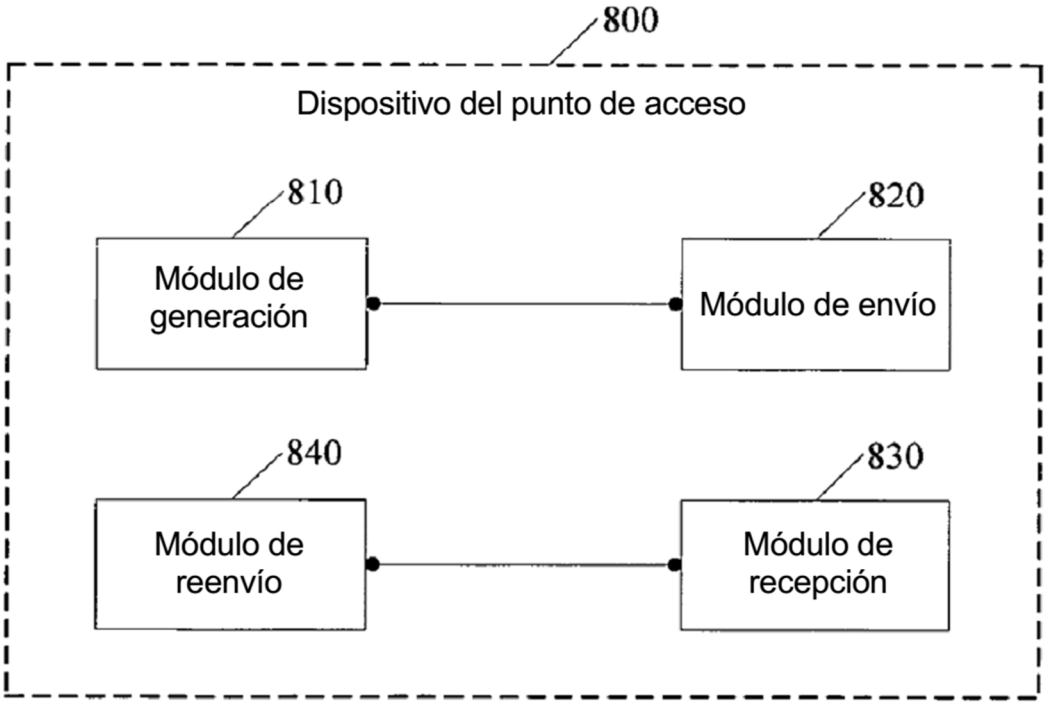
800
Dispositivo del punto de acceso
810
Módulo de generación
820
Módulo de envío
840
Módulo de reenvío
830
Módulo de recepción

FIG. 8

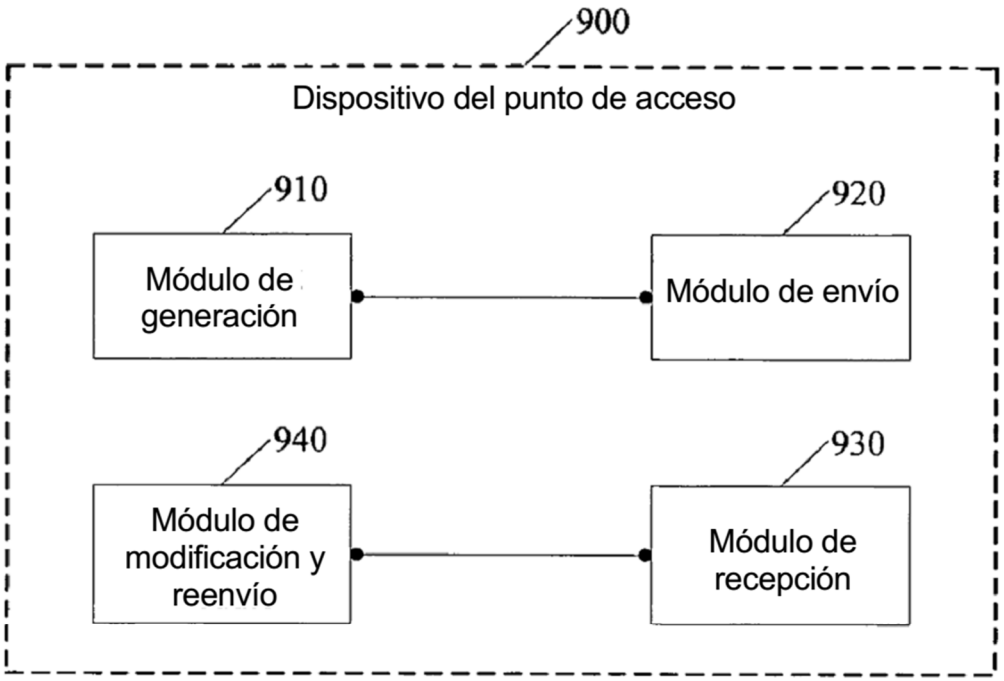

FIG. 9

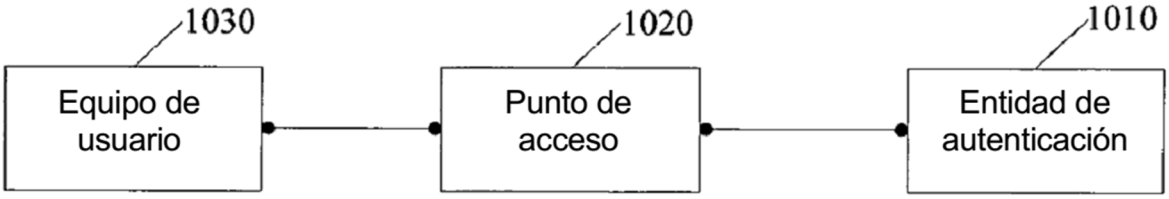

FIG. 10

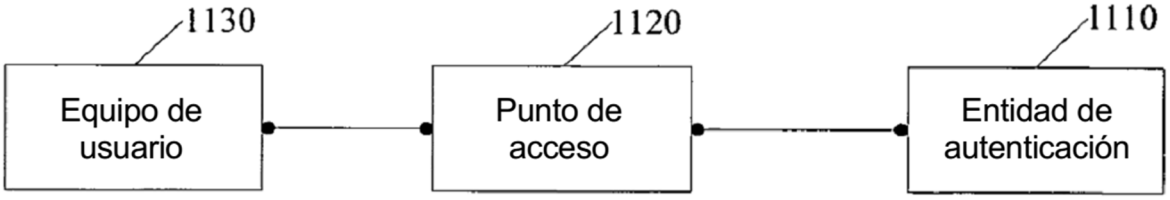

FIG. 11