(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 583 410**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.06.2008 E 14185769 (8)**

(97) Fecha y número de publicación de la concesión europea: **20.04.2016 EP 2838242**

(54) Título: **Método y aparato para impedir que sea falsificada una dirección de control de acceso al soporte en el lado de la red**

(30) Prioridad:

08.06.2007 CN 200710110698

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.09.2016

(73) Titular/es:

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

(72) Inventor/es:

ZHANG, QUN y
KE, BO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

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

DESCRIPCIÓN

Método y aparato para impedir que sea falsificada una dirección de control de acceso al soporte en el lado de la red

CAMPO DE LA INVENCIÓN

La presente invención se refiere a una tecnología de acceso de banda ancha de Internet y al campo de la seguridad de la red y más en particular, a un método y aparato para impedir que sea falsificada una dirección de control de acceso al soporte del lado de la red.

ANTECEDENTES DE LA INVENCIÓN

Con el desarrollo de la tecnología de Internet y la popularización continua de los servicios, se ha desarrollado con rapidez el servicio de acceso de banda ancha. Sin embargo, cómo garantizar la seguridad de los usuarios de banda ancha en la utilización del servicio de banda ancha y la seguridad de operadores de la red es un problema importante que es preciso resolver. A modo de ejemplo, un usuario de acceso falsifica una dirección de control de acceso al soporte (MAC) de un servidor de acceso a distancia de banda ancha (BRAS) para iniciar una aplicación de un protocolo del tipo punto a punto a través de Ethernet (PPPoE) o un protocolo de configuración de host dinámico (DHCP), que causa una migración de una tabla de aprendizaje de dirección MAC del servidor de acceso a distancia de banda ancha (BRAS) en un equipo de acceso desde un puerto del lado de la red a un puerto del lado del usuario y de este modo, se da lugar a la interrupción de los servicios de otros usuarios.

Considerando el modo de desarrollo actual del servicio de banda ancha, un usuario accede a una red para utilizar el servicio de banda ancha en generalmente dos maneras, a saber, autenticación de PPPoE y autenticación de DHCP.

El protocolo PPPoE proporciona un medio de acceso de banda ancha para un usuario que utilice una vía Ethernet puenteada para acceder y al mismo tiempo, proporciona un control del acceso adecuado y su facturación.

El protocolo DHCP se reenvía sobre la base de un protocolo de iniciación del sistema operativo (BOOTP) y su función es proporcionar información de configuración para un concentrador host en la red. El protocolo DHCP emplea un modo de cliente/servidor, en el que un cliente inicia para un servidor una aplicación de configuración que incluye una dirección IP asignada, una máscara de sub-net, una pasarela por defecto y otros parámetros y el servidor reenvía información de configuración correspondiente en conformidad con las políticas establecidas.

Con el fin de resolver el problema de que se falsifique una dirección MAC en el lado de la red, lo que da lugar a que se interrumpa el servicio de otros usuarios del acceso, una función de filtro de direcciones MAC origen está configurada en el puerto del lado del usuario del equipo de acceso en la técnica convencional, esto es, una tabla de filtro de direcciones MAC origen se configura manualmente en el puerto del lado del usuario del equipo de acceso para prohibir a un usuario del acceso utilizar una dirección MAC en la tabla de filtros como una dirección origen. Si el usuario del acceso utiliza una dirección en la tabla de filtrado, el equipo de acceso rechaza el mensaje.

Como puede deducirse del método anterior dado a conocer en la técnica convencional, cuando el servidor BRAS es cambiado o se transfiere un servidor BRAS activo en el lado de la red, la tabla de filtrado de direcciones MAC origen del puerto del lado del usuario necesita ser reconfigurada. La configuración es dependiente de una dirección MAC específica de un equipo de red de capa superior, esto es, la tabla de filtrado de direcciones MAC origen memoriza la dirección MAC del equipo de la capa superior. Si se cambia el equipo de la capa superior, la tabla de filtrado de direcciones MAC origen del equipo de acceso necesita modificarse, lo que origina una importante carga de trabajo de administración y mantenimiento de la red. Puesto que existen un gran número de puertos de usuario de acceso, la función de filtrado de direcciones MAC origen está configurada para los puertos del lado del usuario uno a uno, lo que da lugar a una importante carga de trabajo de mantenimiento del administrador de la red. Por lo tanto, en la creación de la presente invención, el inventor encuentra que la técnica convencional al menos tiene el problema siguiente: una tabla de filtrado de direcciones MAC origen necesita configurarse manualmente en un puerto del lado del usuario del equipo de acceso, lo que da lugar a una importante carga de trabajo de administración y mantenimiento de la red.

El documento US 2006/013221 A1 describe un método para asegurar la comunicación en un conmutador de red de área local (AN) que comprende una interfaz de usuario (UI) y una interfaz de red (NI), comprendiendo las etapas de extracción de una dirección origen (MACi) desde cada paquete recibido por dicho conmutador de red de área local (AN) y la memorización de dicha dirección (MACi) junto con la información asociada en una tabla de reenvío de direcciones (FT).

El documento US 6115376 A describe un método para mejorar la seguridad de la red en una red que incluye un dispositivo de interconexión configurado en estrella tal como un repetidor, un puente o un conmutador, que tiene una pluralidad de puertos adaptados para la conexión a los respectivos dispositivos de la capa de MAC que incluye la memorización de datos de autenticación en el dispositivo de interconexión configurado en estrella que efectúa el mapeado de puesta en correspondencia de las direcciones MAC de las estaciones extremas en la red a puertos

particulares en el dispositivo de interconexión configurado en estrella.

El documento WO 2004/025926 A describe un método para impedir la falsificación de direcciones de red. Se establece un vínculo entre una dirección MAC de protocolo Internet (IP), una dirección de control de acceso al soporte (MAC) y un puerto.

SUMARIO DE LA INVENCIÓN

Con el fin de resolver los problemas técnicos, varias formas de realización de la presente invención dan a conocer un método y aparato para impedir que se falsifique una dirección de control de acceso al soporte (MAC) en el lado de la red, lo que impide automáticamente que sea falsificada la dirección MAC del lado de la red y mejora la conveniencia para administración y mantenimiento.

En una forma de realización, se da a conocer un método para impedir la falsificación de una dirección MAC en el lado de la red. El método incluye las etapas siguientes.

la recepción (101), por un puerto del lado del usuario de un equipo de acceso, un mensaje Discover procedente de un equipo de usuario, UE, y el análisis sintáctico del mensaje Discover procedente del equipo UE para obtener una dirección MAC del equipo UE (102);

el aprendizaje (105), por el equipo de acceso, de la dirección MAC del equipo de usuario UE y el reenvío del mensaje Discover al equipo del lado de la red si la dirección MAC del equipo de usuario UE es diferente de una dirección MAC conocida de un equipo del lado de la red;

la recepción (107), por el equipo de acceso, de un mensaje Offer procedente del equipo del lado de la red, en donde el mensaje Offer comprende una dirección MAC del equipo del lado de la red;

el aprendizaje, por el equipo de acceso, de la dirección MAC del equipo del lado de la red; y

la configuración, por el equipo de acceso, de un circuito integrado lógico del equipo de acceso para utilizar la dirección MAC aprendida para filtrar mensajes que tengan direcciones MAC origen idénticas a la dirección MAC del equipo del lado de la red y procedentes de otros puertos del lado del usuario.

En una forma de realización, se da a conocer un método para impedir que se falsifique una dirección MAC en el lado de la red. El método incluye las etapas siguientes:

la recepción (201), por un puerto del lado del usuario de un mensaje de inicialización de descubrimiento activo de PPPoE, PADI, del equipo de acceso, procedente de un equipo de usuario, UE, y el análisis sintáctico del mensaje PADI del equipo de usuario UE para obtener una dirección MAC del equipo UE (202);

el aprendizaje, por el equipo de acceso, de la dirección MAC del equipo UE y el reenvío del mensaje PADI al equipo del lado de la red si la dirección MAC del equipo de usuario UE es diferente de una dirección MAC conocida de un equipo del lado de la red,

la recepción (207), por el equipo de acceso, de un mensaje de oferta de descubrimiento activo de PPPoE, PADO, procedente del equipo del lado de la red, en donde el mensaje PADO comprende una dirección MAC del equipo del lado de la red;

el aprendizaje, por equipo de acceso, de la dirección MAC del equipo del lado de la red; y

la configuración, por el equipo de acceso, de un circuito integrado lógico del equipo de acceso para utilizar la dirección MAC aprendida para filtrar mensajes que tengan direcciones MAC origen idénticas con la dirección MAC del equipo del lado de la red y procedentes de otros puertos del lado del usuario.

En una forma de realización, se da a conocer un equipo de acceso, comprendiendo dicho equipo de acceso:

una unidad de adquisición (31), configurada para adquirir una dirección MAC de un equipo de usuario, UE, por intermedio de un mensaje de descubrimiento recibido por un puerto del lado del usuario del equipo de acceso;

una unidad de aprendizaje (33), configurada para aprender la dirección MAC del equipo UE si la dirección MAC del equipo UE es diferente de una dirección MAC conocida de un equipo del lado de la red y aprender una dirección MAC del equipo de la red por intermedio de un mensaje Offer enviado desde el equipo del lado de la red;

una unidad de establecimiento (34), configurada para configurar la dirección MAC aprendida en un circuito integrado lógico de una unidad de filtro (37); y

la unidad de filtro (37), configurada para realizar una función de filtrado de direcciones MAC origen por el circuito integrado lógico.

En una forma de realización, se da a conocer un equipo de acceso, en donde el equipo de acceso comprende:

una unidad de adquisición (31), configurada para adquirir una dirección MAC de un equipo de usuario, UE, por intermedio de un mensaje de inicialización de descubrimiento activo de PPPoE, PADI, recibido por un puerto del lado del usuario del equipo de acceso;

una unidad de aprendizaje (33), configurada para aprender la dirección MAC del equipo UE si la dirección MAC del equipo UE es diferente de una dirección MAC conocida de un equipo del lado de la red y para aprender una dirección MAC del equipo de la red por intermedio de un mensaje de oferta de descubrimiento activo de PPPoE, PADO, enviado desde el equipo del lado de la red;

una unidad de establecimiento (34), configurada para configurar la dirección MAC aprendida en un circuito integrado lógico de una unidad de filtro (37); y

la unidad de filtro (37), configurada para realizar una función de filtrado de direcciones MAC origen mediante el circuito integrado lógico.

En una forma de realización, se da a conocer un método para impedir la falsificación de una dirección MAC del lado de la red. El método incluye las etapas siguientes.

Un mensaje procedente de un equipo de usuario (UE) se recibe, y el mensaje del equipo UE se resuelve para obtener una dirección MAC del equipo UE.

La dirección MAC del equipo de usuario UE se aprende si la dirección MAC del equipo de usuario UE es diferente de una dirección MAC conocida de un equipo del lado de la red.

La dirección MAC del equipo del lado de la red es objeto de aprendizaje.

Una tabla de aprendizaje de direcciones MAC se genera utilizando la dirección MAC aprendida del equipo del lado de la red y la tabla de aprendizaje de direcciones MAC generadas se establece para ser una tabla de direcciones estáticas y/o mensajes procedentes de otros puertos del lado del usuario y con direcciones MAC origen siendo la dirección MAC del equipo del lado de la red se filtran utilizando la dirección MAC aprendida del equipo del lado de la red.

En una forma de realización, se da a conocer un aparato para impedir la falsificación de la dirección MAC del lado de la red. Este aparato incluye una unidad de adquisición, una unidad de determinación y una unidad de aprendizaje.

La unidad de adquisición está adaptada para adquirir una dirección MAC de un equipo de usuario UE.

La unidad de determinación está adaptada para determinar si la dirección MAC del equipo de usuario UE que se adquiere por la unidad de adquisición es una dirección MAC conocida de un equipo del lado de la red.

La unidad de aprendizaje está adaptada para aprender la dirección MAC del equipo de usuario UE y la dirección MAC del equipo del lado de la red cuando un resultado de la determinación de la unidad de determinación es que la dirección MAC del equipo de usuario UE no es la dirección MAC conocida del equipo del lado de la red.

El aparato incluye, además, una unidad de generación de tabla de direcciones y/o una unidad de filtro.

La unidad de generación de tabla de direcciones está adaptada para generar una tabla de aprendizaje de direcciones MAC basada en la dirección MAC aprendida del equipo del lado de la red, en donde la tabla de aprendizaje de direcciones MAC se establece para ser una tabla de direcciones MAC estática.

La unidad de filtro está adaptada para filtrar mensajes procedentes de otros puertos del lado del usuario y con direcciones MAC origen siendo la dirección MAC del equipo del lado de la red utilizando la dirección MAC aprendida del equipo del lado de la red.

En una forma de realización, un equipo de acceso que conecta un usuario a una red se da a conocer para obtener servicios de la red. El equipo de acceso incluye una unidad de adquisición, una unidad de determinación y una unidad de aprendizaje.

La unidad de adquisición está adaptada para recibir un mensaje procedente de un equipo de usuario UE y para resolver el mensaje desde el equipo UE para obtener una dirección MAC del equipo de usuario UE.

La unidad de determinación está adaptada para determinar si la dirección MAC del equipo de usuario UE adquirida por la unidad de adquisición es una dirección MAC conocida de un equipo del lado de la red.

La unidad de aprendizaje está adaptada para aprender la dirección MAC del equipo de usuario UE y para aprender la dirección MAC del equipo del lado de la red para generar una tabla de aprendizaje de direcciones MAC que incluye la dirección MAC del equipo del lado de la red cuando un resultado de determinación de la unidad de determinación es que la dirección MAC del equipo de usuario UE no es la dirección MAC conocida del equipo del lado de la red.

El aparato incluye, además, una unidad de generación de tablas de direcciones y/o una unidad de filtro.

La unidad de generación de tabla de direcciones está adaptada para generar la tabla de aprendizaje de direcciones MAC basada en la dirección MAC aprendida del equipo del lado de la red, en donde la tabla de aprendizaje de direcciones MAC se establece para ser una tabla de direcciones MAC estática.

La unidad de filtro está adaptada para filtrar mensajes procedentes de otros puertos del lado del usuario y con direcciones MAC origen que son la dirección MAC del equipo del lado de la red utilizando la dirección MAC aprendida del equipo del lado de la red.

Con el método y aparato para impedir la falsificación de la dirección MAC del lado de la red, dado a conocer en las formas de realización de la presente invención, cuando la dirección MAC del equipo de usuario UE no es la dirección MAC del equipo del lado de la red, se permite al equipo de acceso aprender las direcciones MAC del equipo de usuario UE y del equipo del lado de la red con el fin de impedir que se reubique la tabla de aprendizaje de direcciones MAC, con lo que se impide automáticamente la falsificación por el usuario del equipo del lado de la red para acceder a la red, impidiendo que otros puertos, a partir del aprendizaje de la dirección MAC del equipo del lado de la red, puedan falsificar la dirección MAC del equipo del lado de la red y ser más conveniente para tareas de administración y mantenimiento.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención se entenderá más completamente a partir de la descripción detallada aquí dada a conocer, a continuación, para iluminación solamente, cuando se toma con referencia a los dibujos adjuntos entre los que:

La Figura 1 es un diagrama de flujo de señalización de un método para impedir que una dirección MAC del lado de la red sea falsificada en conformidad con una primera forma de realización de la presente invención;

La Figura 2 es un diagrama de flujo de señalización de un método para impedir que una dirección MAC del lado de la red sea falsificada en conformidad con una segunda forma de realización de la presente invención; y

La Figura 3 es una vista estructural de un aparato para impedir la falsificación de una dirección MAC del lado de la red en conformidad con una forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Con el fin de hacer más clara la solución técnica de la presente invención, se ilustra en detalle, a continuación, mediante formas de realización haciendo referencia a los dibujos adjuntos. La Figura 1 es un diagrama de flujo de señalización de un método para impedir la falsificación de la dirección MAC del lado de la red en conformidad con una primera forma de realización de la presente invención. Un escenario operativo de aplicación de esta forma de realización es que un usuario solicite al equipo del lado de la red la asignación de una dirección IP utilizando la tecnología DHCP y el usuario accede al equipo del lado de la red por primera vez. El proceso principal del método incluye las etapas siguientes.

En la etapa 101, un equipo de usuario UE envía un mensaje Discover a un equipo de acceso para encontrar un servidor DHCP.

En esta forma de realización, el equipo de acceso es un multiplexor de acceso de línea de abonado digital (DSLAM).

En la etapa 102, el equipo de acceso realiza un análisis sintáctico del mensaje Discover recibido para adquirir una dirección MAC origen a partir del mensaje Discover recibido, esto es, una dirección MAC del equipo de usuario UE.

En la etapa 103, se determina si la dirección MAC del equipo de usuario UE adquirida por el equipo de acceso es una dirección MAC conocida del equipo del lado de la red. Si la dirección MAC del equipo de usuario UE es una dirección MAC conocida del equipo del lado de la red, se realiza la etapa 104; de no ser así, se realiza la etapa 105.

La dirección MAC conocida del equipo del lado de la red puede ser una dirección MAC de un equipo del lado de la red registrada en el equipo de acceso. A modo de ejemplo, el equipo de acceso puede adquirir la dirección MAC del

equipo del lado de la red en la red en virtud de un protocolo de enrutamiento o un protocolo de resolución de dirección (ARP) y memorizar la dirección MAC adquirida del equipo del lado de la red en el equipo de acceso. En esta forma de realización, el equipo del lado de la red es el servidor DHCP.

En la etapa 104, el mensaje Discover es rechazo con el fin de impedir que el usuario falsifique la dirección MAC del equipo del lado de la red, a modo de ejemplo, falsificando una dirección MAC de un servidor BRAS.

En la etapa 105, el equipo de acceso aprende la dirección MAC adquirida del equipo de usuario UE.

En la etapa 106, el equipo de acceso reenvía el mensaje Discover al equipo del lado de la red.

En la etapa 107, el equipo del lado de la red reenvía un mensaje Offer al equipo de acceso, con el mensaje Offer incluyendo información del equipo del lado de la red.

La información del equipo del lado de la red incluye una dirección IP del equipo del lado de la red, una dirección MAC del equipo del lado de la red, etc.

En la etapa 108, el equipo de acceso realiza un análisis sintáctico del mensaje Offer recibido para adquirir una dirección MAC origen del mensaje Offer, esto es, una dirección MAC del equipo del lado de la red.

En la etapa 109, el equipo de acceso aprende la dirección MAC del equipo del lado de la red, registra la dirección MAC aprendida del equipo del lado de la red en el equipo de acceso y realiza una operación para impedir que la tabla de aprendizaje de direcciones MAC sea reubicada con el fin de impedir el aprendizaje de la dirección MAC del equipo del lado de la red con procedencia de otros puertos.

La operación de impedir que la tabla de aprendizaje de direcciones MAC sea reubicada específicamente incluye: la generación de la tabla de aprendizaje de direcciones MAC utilizando la dirección MAC del equipo del lado de la red, en donde la tabla de aprendizaje de direcciones MAC se establece para ser una tabla de direcciones MAC estática, de modo que la dirección MAC del equipo del lado de la red le sea impedido suprimir la dirección MAC aprendida en el transcurso del tiempo; y/o configurar un circuito integrado lógico para filtrar mensajes que tienen direcciones MAC origen idénticas con la dirección MAC del equipo del lado de la red y que procedan de otros puertos del lado del usuario utilizando la dirección MAC aprendida del equipo del lado de la red, a modo de ejemplo, estableciendo la dirección MAC aprendida del equipo del lado de la red en una tabla de filtrado de direcciones MAC del circuito integrado lógico o memorizando la dirección MAC aprendida en el equipo de acceso para proporcionar funciones de filtrado y consulta de direcciones MAC.

En la etapa 110, el equipo de acceso reenvía el mensaje Offer al equipo de usuario UE, con el mensaje Offer incluyendo información del equipo del lado de la red.

En la etapa 111, el equipo de usuario UE envía un mensaje de Demanda Request al equipo de acceso para demandar al equipo del lado de la red que asigne una dirección IP para el usuario.

En la etapa 112, el equipo de acceso realiza un análisis sintáctico del mensaje de Demanda Request recibido para adquirir una dirección MAC origen del mensaje Request recibido, esto es, una dirección MAC del equipo de usuario UE.

En la etapa 113, se determina si la dirección MAC del equipo de usuario UE adquirida por el equipo de acceso es la dirección MAC conocida del equipo del lado de la red. Si la dirección MAC del equipo de usuario UE la dirección MAC conocida del equipo del lado de la red, se realiza la etapa 114; de no ser así, se realiza la etapa 115.

En la etapa 114, el mensaje Request se rechaza para impedir la falsificación por el usuario de la dirección MAC del equipo del lado de la red.

En la etapa 115, el equipo de acceso aprender la dirección MAC adquirida del equipo de usuario UE.

En la etapa 116, el equipo de acceso reenvía el mensaje Request al equipo del lado de la red.

En la etapa 117, el equipo del lado de la red asigna una dirección IP para el usuario y reenvía un mensaje de confirmación ACK que incluye la dirección IP asignada para el usuario para el equipo de acceso.

En la etapa 118, el equipo de acceso realiza un análisis sintáctico del mensaje ACK recibido para adquirir una dirección MAC origen del mensaje de confirmación ACK, esto es, una dirección MAC del equipo del lado de la red.

En la etapa 119, el equipo de acceso aprende la dirección MAC del equipo del lado de la red, registra la dirección MAC aprendida del equipo del lado de la red en el equipo de acceso y realiza una operación de impedir que la tabla de aprendizaje de direcciones MAC sea reubicada con el fin de impedir el aprendizaje de la dirección MAC del

equipo del lado de la red procedente de otros puertos.

La operación de impedir que la tabla de aprendizaje de direcciones MAC sea reubicada específicamente incluye: la generación de la tabla de aprendizaje de direcciones MAC utilizando la dirección MAC del equipo del lado de la red, en donde la tabla de aprendizaje de direcciones MAC se establece para ser una tabla de direcciones MAC estática, de modo que la dirección MAC del equipo del lado de la red sea bloqueada para impedir que la dirección MAC aprendida sea suprimida en el transcurso del tiempo; y/o la configuración del circuito integrado lógico para filtrar mensajes que tengan direcciones MAC origen siendo la dirección MAC del equipo del lado de la red y procedentes de otros puertos del lado del usuario utilizando la dirección MAC aprendida del equipo del lado de la red, a modo de ejemplo, estableciendo la dirección MAC aprendida del equipo del lado de la red en una tabla de filtrado de direcciones MAC del circuito integrado lógico o memorizando la dirección MAC aprendida en el equipo de acceso para proporcionar funciones de consulta y filtrado de direcciones MAC.

En la etapa 120, el equipo de acceso reenvía el mensaje ACK al equipo de usuario UE, con el mensaje ACK incluyendo la dirección IP asignada por el equipo del lado de la red para el usuario.

Si el usuario ha realizado satisfactoriamente una autenticación de acceso del equipo del lado de la red con anterioridad, las etapas 101 a 110 pueden omitirse.

La Figura 2 es un diagrama de flujo de señalización de un método para impedir la falsificación de una dirección MAC del lado de la red en conformidad con una segunda forma de realización de la presente invención. Un escenario operativo de aplicación de esta forma de realización es que un usuario demande un establecimiento de una sesión empleando la tecnología PPPoE. El proceso principal del método incluye las etapas siguientes.

En la etapa 201, un equipo de usuario UE envía un mensaje de inicialización de descubrimiento activo de PPPoE (PADI) a un equipo de acceso para demandar servicios de establecimiento de sesión.

En esta forma de realización, el equipo de acceso es un multiplexor de acceso de línea de abonado digital (DSLAM).

En la etapa 202, el equipo de acceso recibe el mensaje PADI procedente del equipo de usuario UE, y realiza el análisis sintáctico del mensaje PADI recibido para adquirir una dirección MAC origen del mensaje PADI recibido, esto es, una dirección MAC del equipo de usuario UE.

En la etapa 203, se determina si la dirección MAC del equipo de usuario UE adquirida por el equipo de acceso es una dirección MAC conocida del equipo del lado de la red. Si la dirección MAC del equipo de usuario UE es una dirección MAC conocida del equipo del lado de la red, se realiza la etapa 204; de no ser así, se realiza la etapa 205.

El equipo de acceso puede aprender una dirección MAC del equipo del lado de la red en virtud de un protocolo de enrutamiento u otros métodos. En esta forma de realización, el equipo del lado de la red es un servidor BRAS.

En la etapa 204, el mensaje PADI se rechaza con el fin de impedir que se falsifique por el usuario la dirección MAC del equipo del lado de la red, a modo de ejemplo, falsificando una dirección MAC del servidor BRAS.

En la etapa 205, el equipo de acceso aprende la dirección MAC adquirida del equipo de usuario UE.

En la etapa 206, el equipo de acceso reenvía el mensaje PADI al equipo del lado de la red.

En la etapa 207, el equipo del lado de la red reenvía un mensaje de oferta de descubrimiento activo de PPPoE (PADO) al equipo de acceso, con el mensaje PADO incluyendo información del equipo del lado de la red.

La información del equipo del lado de la red incluye una dirección MAC del equipo del lado de la red, etc.

En la etapa 208, el equipo de acceso realiza un análisis sintáctico del mensaje PADO recibido para adquirir una dirección MAC origen del mensaje PADO, esto es, una dirección MAC del equipo del lado de la red.

En la etapa 209, el equipo de acceso aprende la dirección MAC del equipo del lado de la red, registral a dirección MAC aprendida del equipo del lado de la red en el equipo de acceso, y realiza una operación de impedir que una tabla de aprendizaje de direcciones MAC sea reubicada con el fin de impedir que la dirección MAC del equipo del lado de la red sea objeto de aprendizaje desde otros puertos.

A modo de ejemplo, puede generarse una tabla de aprendizaje de direcciones MAC estática, o un circuito integrado lógico puede configurarse de modo que el circuito integrado lógico filtre mensajes que tengan direcciones MAC origen idénticas con la dirección MAC del equipo del lado de la red y procedan de otros puertos del lado del usuario utilizando la dirección MAC aprendida del equipo del lado de la red o la tabla de direcciones MAC generada.

En la etapa 210, el equipo de acceso reenvía el mensaje PADO al equipo de usuario UE, con el mensaje PADO

incluyendo información del equipo del lado de la red.

En la etapa 211, el equipo de usuario UE envía un mensaje de demanda de descubrimiento activo de PPPoE (PADR) al equipo de acceso para demandar los servicios de establecimiento de sesión.

En la etapa 212, el equipo de acceso realiza un análisis sintáctico del mensaje PADR recibido para adquirir una dirección MAC origen del mensaje PADR recibido, esto es, una dirección MAC del equipo de usuario UE.

En la etapa 213, se determina si la dirección MAC del equipo de usuario UE adquirida por el equipo de acceso es la dirección MAC conocida del equipo del lado de la red. Si el equipo de acceso es una dirección MAC conocida del equipo del lado de la red, se realiza la etapa 214; de no ser así, se realiza la etapa 215.

En la etapa 214, el mensaje PADR se rechaza con el fin de impedir la falsificación por el usuario de la dirección MAC del equipo del lado de la red.

En la etapa 215, el equipo de acceso aprende la dirección MAC adquirida del equipo de usuario UE.

En la etapa 216, el equipo de acceso reenvía el mensaje PADR al equipo del lado de la red.

En la etapa 217, el equipo del lado de la red proporciona una conexión de establecimiento de servicio de sesión al usuario y reenvía un mensaje de confirmación-sesión de descubrimiento activo de PPPoE (PADS) al equipo de acceso.

En la etapa 218, el equipo de acceso realiza el análisis del mensaje PADS recibido para adquirir una dirección MAC origen del mensaje PADS, esto es, una dirección MAC del equipo del lado de la red.

En la etapa 219, el equipo de acceso aprende la dirección MAC del equipo del lado de la red, genera la tabla de aprendizaje de direcciones MAC y realiza una operación para impedir que la tabla de aprendizaje de direcciones MAC sea reubicada con el fin de impedir que la dirección MAC del equipo del lado de la red sea objeto de aprendizaje desde otros puertos.

A modo de ejemplo, la tabla de aprendizaje de direcciones MAC puede establecerse para ser una tabla de direcciones MAC estática, de modo que la dirección MAC del equipo del lado de la red sea bloqueada para impedir que la dirección MAC aprendida del equipo del lado de la red sea suprimida en el transcurso del tiempo y/o un circuito integrado lógico está configurado para filtrar mensajes que tengan direcciones MAC origen idénticas con la dirección MAC del equipo del lado de la red y procedentes de otros puertos del lado del usuario utilizando la dirección MAC aprendida del equipo del lado de la red o la tabla de direcciones MAC generada que incluye la dirección MAC del equipo del lado de la red.

En la etapa 220, el equipo de acceso reenvía el mensaje PADS al usuario.

La Figura 3 es una vista estructural de un aparato para impedir que una dirección MAC del lado de la red sea falsificada en conformidad con una forma de realización de la presente invención.

El aparato incluye una unidad de adquisición 31, una unidad de determinación 32, una unidad de aprendizaje 33 y puede incluir, además, una unidad de establecimiento 34, una unidad de memorización 35, una unidad de generación de tabla de direcciones 36 y una unidad de filtro 37.

La unidad de adquisición 31 está adaptada para adquirir y memorizar una dirección MAC de un equipo de usuario UE. La unidad de memorización 35 está adaptada para memorizar una dirección MAC adquirida del equipo del lado de la red. La unidad de determinación 32 está adaptada para determinar si la dirección MAC del equipo de usuario UE adquirida por la unidad de adquisición 31 es la dirección MAC del equipo del lado de la red que se memoriza en la unidad de memorización 35. La unidad de aprendizaje 33 está adaptada para aprender la dirección MAC del equipo de usuario UE y la dirección MAC del equipo del lado de la red cuando un resultado de determinación de la unidad de determinación 32 es que la dirección MAC del equipo de usuario UE no es la dirección MAC del equipo del lado de la red. Más concretamente, la dirección MAC del equipo del lado de la red puede ser objeto de aprendizaje en al menos una de las maneras operativas siguientes: adquiriendo la dirección MAC del equipo del lado de la red mediante un protocolo de enrutamiento; adquiriendo la dirección MAC del equipo del lado de la red mediante un ARP; y adquiriendo la dirección MAC del equipo del lado de la red a partir de un mensaje de respuesta del equipo del lado de la red. La unidad de generación de tabla de direcciones 36 está adaptada para generar una tabla de aprendizaje de direcciones MAC utilizando la dirección MAC aprendida por la unidad de aprendizaje 33. La unidad de establecimiento 34 está adaptada para establecer la tabla de aprendizaje de direcciones MAC para ser una tabla de direcciones MAC estática con el fin de impedir que la tabla de aprendizaje de direcciones MAC generada por la unidad de aprendizaje 33 sea objeto de reubicación. La unidad de establecimiento 34 puede configurar también la dirección MAC del lado de la red aprendida en la unidad de filtro 37. La unidad de filtro 37 realiza una función de filtrado de direcciones MAC origen mediante un circuito integrado lógico. El circuito integrado

lógico de la unidad de filtro 37 registra una tabla de filtrado de direcciones MAC y puede configurarse para filtrar mensajes que tengan direcciones MAC origen que sean la dirección MAC del equipo del lado de la red y procedente de otros puertos del lado del usuario utilizando la tabla de filtrado de direcciones MAC. O bien, a modo de ejemplo, la unidad de filtro 37 puede tener una función de motor para obtener mediante consulta de la dirección MAC del equipo del lado de la red procedente de la tabla de aprendizaje de direcciones MAC con el fin de ser filtrada. La unidad de generación de tabla de direcciones 36 puede configurarse para establecer directamente un atributo de la tabla de aprendizaje de direcciones MAC para ser estática durante la generación de la tabla de aprendizaje de direcciones MAC en conformidad con la dirección MAC aprendida del equipo de red.

Haciendo referencia a las Figuras 1, 2 y 3, el sistema de comunicaciones dado a conocer en las formas de realización de la presente invención incluye el equipo de acceso, el equipo de usuario UE y el equipo del lado de la red. El equipo de acceso está adaptado principalmente para proporcionar una diversidad de medios de acceso para acceder el usuario a la red con el fin de adquirir servicios de la red. El equipo de usuario UE está principalmente adaptado para proporcionar una función de cliente de acceso del usuario. El equipo del lado de la red está adaptado principalmente para proporcionar información pertinente de los servicios de la red.

El equipo de acceso, a modo de ejemplo, el DSLAM, proporciona un puerto del lado del usuario y un puerto del lado de la red. El puerto del lado del usuario está adaptado para la conexión del usuario y el puerto del lado de la red está conectado a una red de área local (LAN), una red de área metropolitana (MAN) o una red base. El equipo de acceso tiene tablas de direcciones memorizadas e incluye una tabla de direcciones estática y una tabla de direcciones dinámica. La tabla de direcciones estática suele estar configurada en el equipo manualmente y está caracterizada por cuanto que la tabla se memoriza en el equipo en todo momento una vez que esté configurada y no sea suprimida en el transcurso del tiempo. La tabla de direcciones dinámica se suele generar por el equipo mediante un aprendizaje automático y se caracteriza por cuanto que la tabla se suprime automáticamente después de memorizarse en el equipo durante un periodo de tiempo. En conformidad con las formas de realización de la presente invención, el equipo de acceso puede generar la tabla de direcciones MAC estática en conformidad con la dirección MAC del lado de la red aprendida con el fin de impedir que la tabla de aprendizaje de direcciones MAC sea objeto de reubicación, y/o el equipo de acceso puede configurarse para filtrar mensajes que tengan direcciones MAC origen que sean la dirección MAC del equipo del lado de la red y procedentes de otros puertos del lado del usuario utilizando la dirección MAC aprendida del equipo del lado de la red. El equipo de acceso puede aprender la dirección MAC del equipo del lado de la red en al menos una de las maneras operativas siguientes: adquisición de la dirección MAC del equipo del lado de la red mediante un protocolo de enrutamiento; la adquisición de la dirección MAC del equipo del lado de la red por un ARP; y la recepción de un mensaje de respuesta del equipo del lado de la red y la adquisición de la dirección MAC del equipo del lado de la red.

El equipo del lado de la red es, a modo de ejemplo, el servidor DHCP ilustrado en la Figura 1 y el servidor BRAS ilustrado en la Figura 2. Según se ilustra en la Figura 1, un modo de servidor/cliente se utiliza entre el servidor DHCP y el equipo de usuario UE, en donde un cliente presenta a un servidor una solicitud de configuración incluyendo la dirección IP asignada, una máscara de sub-red, una pasarela por defecto y otros parámetros, y el servidor reenvía la información de configuración correspondiente incluyendo la dirección IP asignada, la máscara de sub-red, la pasarela por defecto y otros parámetros en conformidad con las políticas establecidas. Con el método y aparato anteriores para impedir automáticamente que se falsifique la dirección MAC del lado de la red, dados a conocer en las formas de realización de la presente invención, solamente cuando la dirección MAC del equipo de usuario UE no es la dirección MAC del equipo del lado de la red, al equipo de acceso le está permitido aprender las direcciones MAC del equipo de usuario UE y el equipo del lado de la red para impedir que la tabla de aprendizaje de direcciones MAC sea objeto de reubicación, con lo que se impide que el usuario falsifique el equipo del lado de la red para acceder a la red, con lo que se impide el aprendizaje de la dirección MAC del equipo del lado de la red procedente de otros puertos para falsificar la dirección MAC del equipo del lado de la red y ser más conveniente para las tareas de administración y mantenimiento.

Un método y aparato para impedir que se falsifique la dirección MAC del lado de la red, dados a conocer en la presente invención, se describieron en detalle con anterioridad. Instancias operativas específicas se aplican en esta descripción para elaborar los principios y la puesta en práctica de la presente invención, pero la ilustración de las formas de realización anteriores está simplemente prevista para ayudar a entender las soluciones técnicas dadas a conocer en la presente invención. Asimismo, es evidente para los expertos en esta técnica que se pueden realizar cambios en la puesta en práctica específica y el alcance de aplicación de la presente invención sobre la base del concepto de la invención. Considerando lo que antecede, los contenidos de la especificación no se considerarán como una limitación de la presente invención.

REIVINDICACIONES

1. Un método para impedir que sea falsificada una dirección de control de acceso al soporte, MAC, del lado de la red que comprende:

la recepción (101), por un puerto del lado del usuario perteneciente a un equipo de acceso, de un mensaje Discover procedente de un equipo de usuario, UE, y el análisis sintáctico del mensaje Discover del UE para obtener una dirección MAC del equipo UE (102), caracterizado por cuanto que el método comprende, además:

el aprendizaje (105), por el equipo de acceso, de la dirección MAC del equipo de usuario UE y el reenvío del mensaje Discover al equipo del lado de la red si la dirección MAC del equipo UE es diferente de una dirección MAC conocida de un equipo del lado de la red;

la recepción (107), por el equipo de acceso, de un mensaje Offer procedente del equipo del lado de la red, en donde el mensaje Offer incluye una dirección MAC del equipo del lado de la red;

el aprendizaje, por el equipo de acceso, de la dirección MAC del equipo del lado de la red; y

la configuración, por el equipo de acceso, de un circuito integrado lógico del equipo de acceso para utilizar la dirección MAC aprendida con el fin de filtrar mensajes que contienen direcciones MAC origen idénticas con la dirección MAC del equipo del lado de la red y que proceden de otros puertos del lado del usuario.

2. El método según la reivindicación 1, que comprende, además:

el rechazo del mensaje Discover del equipo de usuario UE si la dirección MAC del equipo de usuario UE es la misma que la dirección MAC conocida del equipo del lado de la red.

3. Un método para impedir que sea falsificada una dirección de control de acceso al soporte, MAC, del lado de la red, que comprende:

la recepción (201), por un puerto del lado del usuario perteneciente a un equipo de acceso, de un mensaje de inicialización de descubrimiento activo al protocolo PPPoE, PADI, procedente de un equipo de usuario UE, y el análisis sintáctico del mensaje de inicialización PADI del equipo de usuario UE con el fin de obtener una dirección MAC del equipo de usuario UE (202), caracterizado por cuanto que el método comprende, además:

el aprendizaje, por el equipo de acceso, de la dirección MAC del equipo de usuario UE y el reenvío del mensaje de inicialización PADI hacia el equipo del lado de la red si la dirección MAC del equipo de usuario UE es diferente de una dirección MAC conocida de un equipo del lado de la red;

la recepción (207), por el equipo de acceso, de un mensaje de oferta de descubrimiento activo al protocolo PPPoE, PADO, procedente del equipo del lado de la red, en donde el mensaje PADO comprende una dirección MAC perteneciente al equipo del lado de la red;

el aprendizaje, por el equipo de acceso, de la dirección MAC del equipo del lado de la red; y

la configuración, por el equipo de acceso, de un circuito integrado lógico del equipo de acceso para utilizar la dirección MAC aprendida para filtrar mensajes que tengan direcciones MAC origen idénticas con la dirección MAC del equipo del lado de la red y que procedan de otros puertos del lado del usuario.

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

rechazar, por el equipo de acceso, el mensaje PADI si la dirección MAC del equipo de usuario UE es la misma que la dirección MAC conocida del equipo del lado de la red.

5. Un equipo de acceso, que comprende:

una unidad de adquisición (31), configurada para adquirir una dirección MAC de un equipo de usuario, UE, por intermedio de un mensaje Discover recibido por un puerto del lado del usuario del equipo de acceso y enviado a partir del equipo de usuario UE, caracterizado por cuanto que el equipo de acceso comprende, además:

una unidad de aprendizaje (33), configurada para aprender la dirección MAC del equipo de usuario UE si la dirección MAC del equipo de usuario UE es diferente de una dirección MAC conocida de un equipo del lado de la red y para aprender una dirección MAC del equipo del lado de la red por intermedio de un mensaje Offer enviado a partir del equipo del lado de la red;

una unidad de establecimiento (34), configurada para configurar la dirección MAC aprendida en un circuito integrado

lógico de una unidad de filtro (37); y

la unidad de filtro (37), configurada para realizar una función de filtrado de dirección MAC origen gracias al circuito integrado lógico, con el objeto de filtrar mensajes que tengan una dirección MAC origen idéntica a la dirección MAC del equipo del lado de la red y que procedan de otros puertos del lado del usuario.

6. El equipo de acceso según la reivindicación 5, en donde el circuito integrado lógico de la unidad de filtro (37) filtra los mensajes que tengan direcciones MAC origen que sean idénticas a la dirección MAC del equipo del lado de la red y procedente de otros puertos del lado del usuario utilizando una tabla de filtrado de direcciones MAC.

7. El equipo de acceso según la reivindicación 5 o 6, en donde el equipo de acceso es un Multiplexor de Acceso de Línea de Abonado Digital.

8. Un equipo de acceso que comprende:

una unidad de adquisición (31), configurada para adquirir una dirección MAC de un equipo de usuario, UE, por intermedio de un mensaje de inicialización de descubrimiento activo de PPPoE, PADI, recibido por un puerto del lado del usuario del equipo de acceso y enviado desde el equipo de usuario UE, caracterizado por cuanto que el equipo de acceso comprende, además:

una unidad de aprendizaje (33), configurada para aprender la dirección MAC del equipo de usuario UE si la dirección MAC del equipo de usuario UE es diferente de una dirección MAC conocida de un equipo del lado de la red y para aprender una dirección MAC del equipo de la red por intermedio de un mensaje de oferta de descubrimiento activo de PPPoE, PADO, enviado desde el equipo del lado de la red;

una unidad de establecimiento (34), configurada para configurar la dirección MAC aprendida en un circuito integrado lógico de una unidad de filtro (37); y

la unidad de filtro (37), configurada para realizar una función de filtro de dirección MAC origen mediante el circuito integrado lógico, con el fin de filtrar mensajes que tengan una dirección MAC origen idéntica con la dirección MAC del equipo del lado de la red y las que proceden de otros puertos del lado del usuario.

9. El equipo de acceso según la reivindicación 8, en donde el circuito integrado lógico de la unidad de filtro (37) filtra mensajes que tengan direcciones MAC origen que sean la dirección MAC del equipo del lado de la red y procedentes de otros puertos del lado del usuario utilizando una tabla de filtrado de direcciones MAC.

10. El equipo de acceso según la reivindicación 8 o 9, en donde el equipo de acceso es un Multiplexor de Acceso de Línea de Abonado Digital.

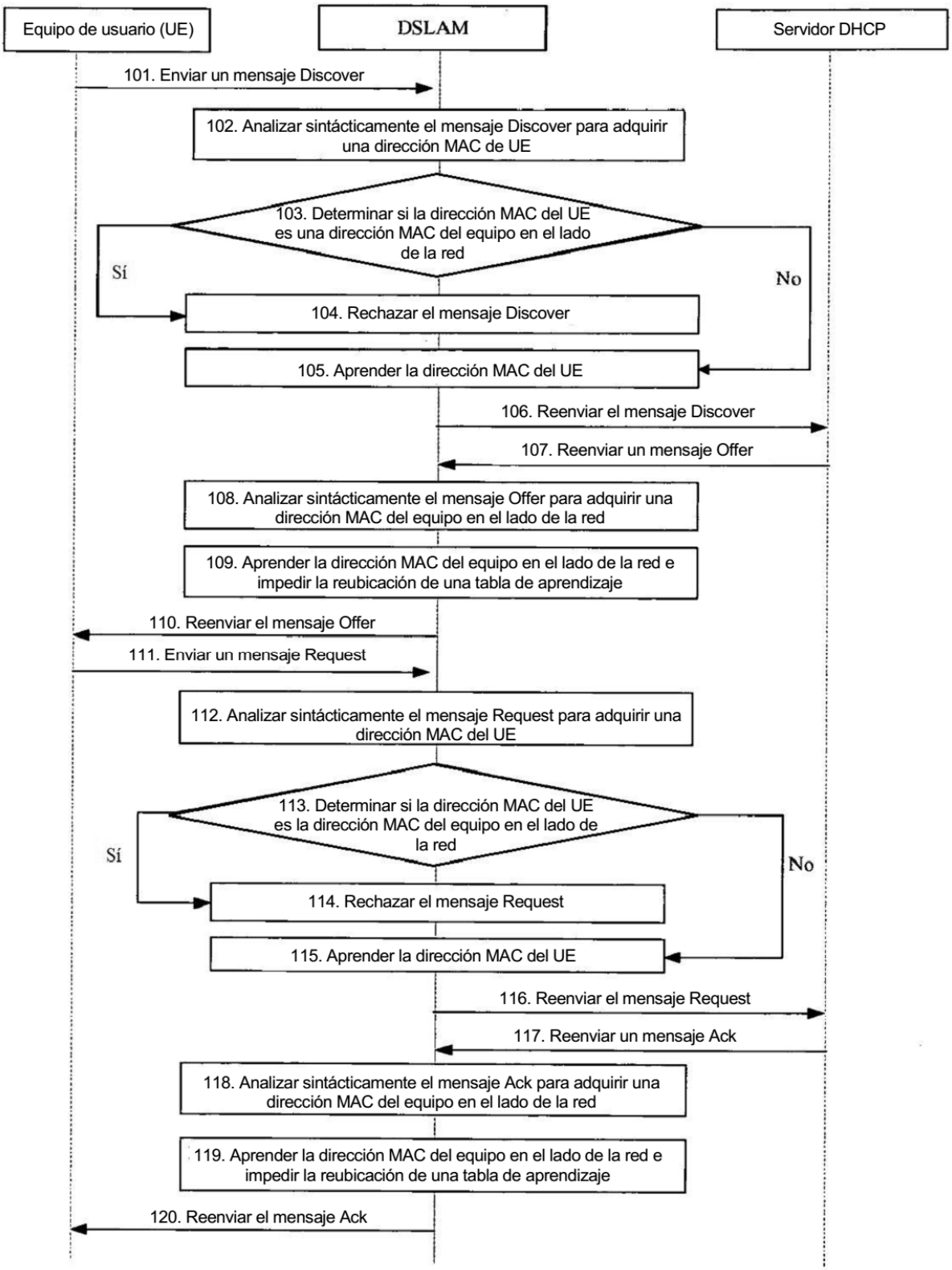
Equipo de usuario (UE)
DSLAM
Servidor DHCP
101. Enviar un mensaje Discover
102. Analizar sintácticamente el mensaje Discover para adquirir una dirección MAC de UE
103. Determinar si la dirección MAC del UE es una dirección MAC del equipo en el lado de la red
Sí
No
104. Rechazar el mensaje Discover
105. Aprender la dirección MAC del UE
106. Reenviar el mensaje Discover
107. Reenviar un mensaje Offer
108. Analizar sintácticamente el mensaje Offer para adquirir una dirección MAC del equipo en el lado de la red
109. Aprender la dirección MAC del equipo en el lado de la red e impedir la reubicación de una tabla de aprendizaje
110. Reenviar el mensaje Offer
111. Enviar un mensaje Request
112. Analizar sintácticamente el mensaje Request para adquirir una dirección MAC del UE
113. Determinar si la dirección MAC del UE es la dirección MAC del equipo en el lado de la red
Sí
No
114. Rechazar el mensaje Request
115. Aprender la dirección MAC del UE
116. Reenviar el mensaje Request
117. Reenviar un mensaje Ack
118. Analizar sintácticamente el mensaje Ack para adquirir una dirección MAC del equipo en el lado de la red
119. Aprender la dirección MAC del equipo en el lado de la red e impedir la reubicación de una tabla de aprendizaje
120. Reenviar el mensaje Ack

FIG. 1

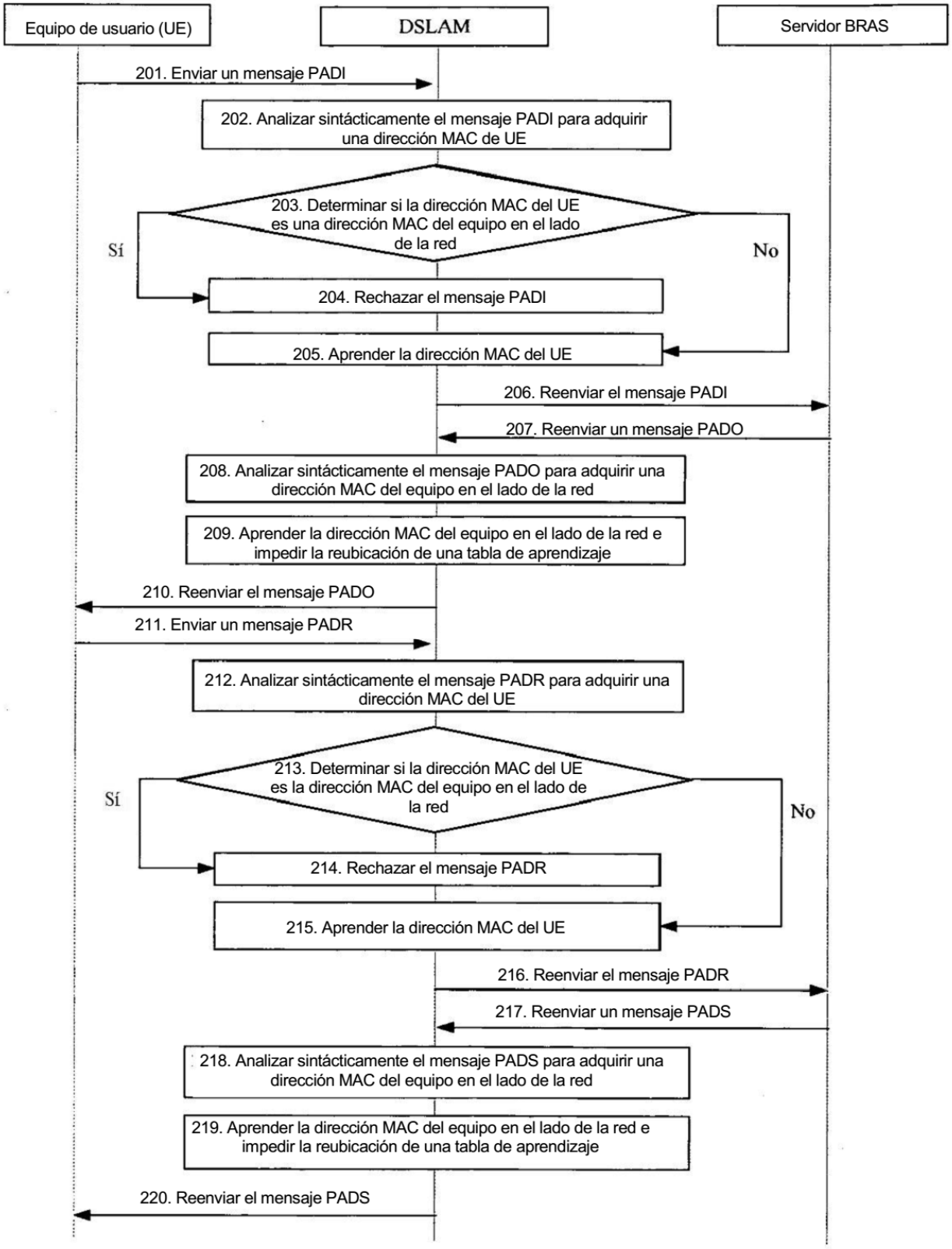
Equipo de usuario (UE)
DSLAM
Servidor BRAS
201. Enviar un mensaje PADI
202. Analizar sintácticamente el mensaje PADI para adquirir una dirección MAC de UE
203. Determinar si la dirección MAC del UE es una dirección MAC del equipo en el lado de la red
Sí
No
204. Rechazar el mensaje PADI
205. Aprender la dirección MAC del UE
206. Reenviar el mensaje PADI
207. Reenviar un mensaje PADO
208. Analizar sintácticamente el mensaje PADO para adquirir una dirección MAC del equipo en el lado de la red
209. Aprender la dirección MAC del equipo en el lado de la red e impedir la reubicación de una tabla de aprendizaje
210. Reenviar el mensaje PADO
211. Enviar un mensaje PADR
212. Analizar sintácticamente el mensaje PADR para adquirir una dirección MAC del UE
213. Determinar si la dirección MAC del UE es la dirección MAC del equipo en el lado de la red
Sí
No
214. Rechazar el mensaje PADR
215. Aprender la dirección MAC del UE
216. Reenviar el mensaje PADR
217. Reenviar un mensaje PADS
218. Analizar sintácticamente el mensaje PADS para adquirir una dirección MAC del equipo en el lado de la red
219. Aprender la dirección MAC del equipo en el lado de la red e impedir la reubicación de una tabla de aprendizaje
220. Reenviar el mensaje PADS

FIG. 2

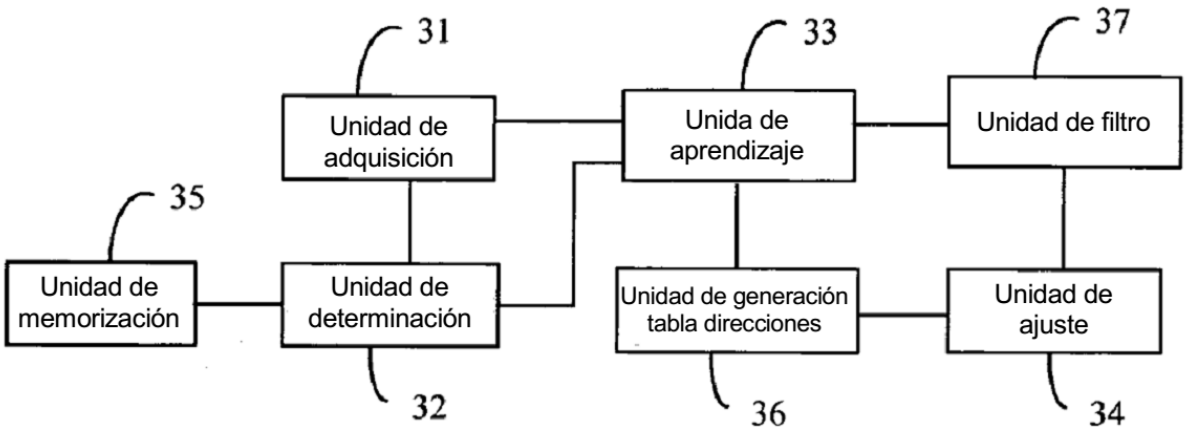
31
33
37
Unidad de adquisición
Unida de aprendizaje
Unidad de filtro
35
Unidad de memorización
Unidad de determinación
Unidad de generación tabla direcciones
Unidad de ajuste
32
36
34

FIG. 3