(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 527 132**

(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 08757607 (0)**

(97) Fecha y número de publicación de la concesión europea: **22.10.2014 EP 2093949**

(54) Título: **Método y dispositivo para impedir que una dirección de control de acceso del medio en el lado de la red sea falseada**

(30) Prioridad:

08.06.2007 CN 200710110698

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.01.2015

(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

DESCRIPCIÓN

Método y dispositivo para impedir que una dirección de control de acceso del medio en el lado de la red sea falseada

Campo de la tecnología

La presente invención está relacionada con una tecnología de acceso de banda ancha en Internet y con el campo de la seguridad de la red y, más en particular, con un método y un dispositivo para impedir que una dirección de control de acceso del medio en el lado de la red sea falseada.

Antecedentes

Con la madurez de las tecnologías de Internet y la continua popularización de los servicios, se ha desarrollado rápidamente el servicio de acceso de banda ancha. Sin embargo, el problema clave a resolver es cómo asegurar la seguridad del usuario de banda ancha al utilizar los servicios de banda ancha y la seguridad de los operadores de la red. Por ejemplo, un usuario de acceso falsifica una dirección del control de acceso al medio (MAC) de un servidor de acceso remoto de banda ancha (BRAS) para iniciar la aplicación de un protocolo de punto a punto sobre Ethernet (PPPoE) o un protocolo dinámico de configuración del ordenador central (DHCP), lo cual origina una migración de una tabla de aprendizaje de direcciones MAC del servidor de acceso remoto de banda ancha (BRAS) sobre un equipo de acceso, desde un puerto del lado de la red a un puerto del lado del usuario y, por tanto, esto da como resultado la interrupción de otros servicios de usuario.

Considerando el modo de desarrollo actual del servicio de banda ancha, un usuario accede a una red para usar el servicio de banda ancha generalmente de dos maneras, es decir, la autenticación del PPPoE y la autenticación del DHCP.

El protocolo PPPoE proporciona un medio de acceso de banda ancha para un usuario que utilice un Ethernet en puente para acceder, y entre tanto proporciona un control y facturación de acceso convenientes.

Se propone el protocolo DHCP sobre la base de un protocolo de arranque (BOOTP), y su función es proporcionar información de configuración para un ordenador central de la red. El DHCP emplea un modo cliente/servidor, en el cual un cliente inicia en un servidor una aplicación de configuración que incluye una dirección de IP asignada, una máscara de sub-red, una pasarela predeterminada y otros parámetros, y el servidor devuelve la correspondiente información de configuración de acuerdo con las políticas.

Con el fin de resolver el problema de que se pueda falsificar una dirección MAC del lado de la red, lo que da como resultado que se interrumpe el servicio de otros usuarios de acceso, se configura una función de filtrado de direcciones MAC de la fuente en el puerto del lado del usuario del equipo de acceso, en la técnica convencional, es decir, se configura manualmente una tabla de filtrado de direcciones MAC de la fuente en el puerto del lado del usuario del equipo de acceso, para prohibir que un usuario de acceso utilice la dirección MAC de la tabla de filtrado como dirección fuente. Si el usuario de acceso utiliza una dirección de la tabla de filtrado, el equipo de acceso descarta el mensaje.

Como puede verse por el método anterior proporcionado en la técnica convencional, cuando se cambia el BRAS o se conmuta un BRAS activo en el lado de la red, necesita reconfigurarse la tabla de filtrado de direcciones MAC de la fuente del puerto del lado de usuario. La configuración depende de la dirección MAC específica de un equipo de red de capa superior, es decir, la tabla de filtrado de direcciones MAC almacena la dirección MAC de la fuente del equipo de la capa superior. Si se cambia equipo de la capa superior, la tabla de filtrado de direcciones MAC de la fuente del equipo de acceso necesita modificarse, lo cual origina una gran sobrecarga de administración y mantenimiento de la red. Como existe una gran número de puertos de usuarios de acceso, la función de filtrado de direcciones MAC de la fuente se configura en los puertos del lado de usuario uno por uno, lo cual origina una gran carga de trabajo de mantenimiento del administrador de la red. Por tanto, en la creación de la presente invención, el inventor se encuentra con que la técnica convencional tiene al menos el problema siguiente: se necesita configurar manualmente una tabla de filtrado de direcciones MAC de la fuente en un puerto del lado de usuario, lo cual origina una gran carga de trabajo de administración y mantenimiento de la red.

El documento US 6115376 A (SHERER W PAUL [US] ET AL) divulga 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 interruptor, que tiene una pluralidad de puertos adaptados para la conexión a respectivos dispositivos de capa MAC, que incluyen datos de autenticación del almacenamiento en el dispositivo de interconexión configurado en estrella que establece una correspondencia entre la dirección MAC de las estaciones finales de la red, con puertos particulares del dispositivo de interconexión configurado en estrella.

El documento WO 2004/025926 A (CISCO TECH IND [US]) divulga un método para impedir la puesta en cola de direcciones de red.

El documento D7 (US 2006/013221 A1 (DE CNODDER STEFAAN J [BE] ET AL DE CNODDER STEFAAN JOZEF [BE] ET AL) 19 Enero 2006) divulga una solución de utilización de direcciones fuente del lado de la red para filtrar nuevas direcciones fuente recibidas en el lado del usuario, si ocurre que la dirección fuente del lado de usuario ya estaba almacenada como dirección fuente del lado de la red, el paquete que contiene la nueva dirección fuente se descarta; en otro caso, se tomará nota de la nueva dirección en el lado del usuario.

Todos estos documentos no muestran ni sugieren ninguna solución para resolver el problema técnico anteriormente descrito.

Sumario

Con el fin de resolver los problemas técnicos, diversos modos de realización de la presente invención proporcionan un método y un dispositivo para impedir que se falsifique una dirección de control de acceso al medio (MAC) en el lado de la red, lo cual impide automáticamente que se falsifique una dirección MAC del lado de la red y refuerza la comodidad de la administración y el mantenimiento.

En un modo de realización, se proporciona un método para impedir que una dirección MAC del lado de la red sea falsificada, como se define en la reivindicación 1.

En un modo de realización, se proporciona un dispositivo para impedir que se falsifique una dirección MAC del lado de la red, como se define en la reivindicación 4.

Con el método y dispositivo para impedir que se falsifique una dirección MAC del lado de la red en los modos de realización proporcionados en la presente invención, cuando la dirección MAC del UE no es la dirección MAC del equipo de red, se permite que el equipo de acceso aprenda las direcciones MAC del UE y del equipo del lado de la red, para impedir que se relocalice la tabla de aprendizaje de direcciones MAC, impidiendo automáticamente con ello que el usuario falsifique el equipo del lado de la red para acceder a la red, impidiendo que otros puertos aprendan la dirección MAC del equipo del lado de la red para falsificar la dirección MAC del equipo del lado de la red y para ser más cómodo de administrar y mantener.

Breve descripción de los dibujos

La presente invención se comprenderá mejor a partir de la siguiente descripción detallada ofrecida a continuación solamente como ilustración, cuando se toma en conjunto con los dibujos que se acompañan, entre los cuales:

La figura 1 es un diagrama de flujo de señalización de un método para impedir que una MAC del lado de la red

por la unidad de adquisición sea una dirección MAC conocida del equipo del lado de la red.

La unidad de aprendizaje está adaptada para aprender la dirección MAC del UE y aprender la dirección MAC del equipo del lado de la red, para generar una tabla de aprendizaje de direcciones MAC que incluya la dirección MAC del equipo del lado de la red, cuando el resultado del juicio que hace la unidad de juicio es que la dirección MAC del UE no es la dirección MAC conocida del equipo del lado de la red.

El dispositivo incluye además una unidad de generación de tablas de direcciones y/o una unidad de filtrado.

La unidad de generación de tablas de direcciones está adaptada para generar la tabla de aprendizaje de direcciones MAC basándose en la dirección MAC aprendida del equipo del lado de la red, en la cual la tabla de aprendizaje de direcciones MAC se fija en una tabla estática de direcciones MAC.

La unidad de filtrado está adaptada para filtrar mensajes desde otros puertos del lado de usuario y siendo las direcciones MAC de la fuente 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 dispositivo para impedir que se falsifique una dirección MAC del lado de la red en los modos de realización proporcionados en la presente invención, cuando la dirección MAC del UE no es la dirección MAC del equipo de red, se permite que el equipo de acceso aprenda las direcciones MAC del UE y del equipo del lado de la red, para impedir que se relocalice la tabla de aprendizaje de direcciones MAC, impidiendo automáticamente con ello que el usuario falsifique el equipo del lado de la red para acceder a la red, impidiendo que otros puertos aprendan la dirección MAC del equipo del lado de la red para falsificar la dirección MAC del equipo del lado de la red y para ser más cómodo de administrar y mantener.

Breve descripción de los dibujos

La presente invención se comprenderá mejor a partir de la siguiente descripción detallada ofrecida a continuación solamente como ilustración, cuando se toma en conjunto con los dibujos que se acompañan, entre los cuales:

La figura 1 es un diagrama de flujo de señalización de un método para impedir que se falsifique una dirección MAC del lado de la red, de acuerdo con un primer modo 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, de acuerdo con un segundo modo de realización de la presente invención, y

La figura 3 es una vista estructural de un dispositivo para impedir que se falsifique una dirección MAC del lado de la red, de acuerdo con un modo de realización de la presente invención.

Descripción detallada

Con el fin de clarificar la solución técnica de la presente invención, a continuación se ilustra con detalle la presente invención a través de los modos de realización, con referencia a los dibujos que se acompañan. La figura 1 es un diagrama de flujo de señalización de un método para impedir que se falsifique una dirección MAC del lado de la red, de acuerdo con un primer modo de realización de la presente invención. Un escenario de aplicación de este modo de realización es que un usuario aplica a un equipo del lado de la red la asignación de una dirección IP empleando la tecnología DHCP, y el usuario accede al equipo del lado de la red por primera vez. El proceso principal del método incluye los pasos siguientes:

En el paso 101, un UE envía un mensaje “Discover” (Descubrir) a un equipo de acceso para encontrar un servidor DHCP.

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

En el paso 102, el equipo de acceso analiza el mensaje Discover recibido para adquirir una dirección MAC de la fuente del mensaje Discover recibido, es decir, una dirección MAC del UE.

En el paso 103, se juzga si la dirección MAC del UE adquirida por el equipo de acceso es una dirección MAC conocida del equipo del lado de la red. Si la dirección MAC del UE es una dirección MAC conocida por el equipo del lado de la red, se efectúa el paso 104; en otro caso, se efectúa el paso 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 grabada en el equipo de acceso. Por 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 encaminamiento o un protocolo de resolución de direcciones (ARP), y almacenar la dirección MAC adquirida del equipo del lado de la red en el equipo de acceso. En este modo de realización, el equipo del lado de la red es el servidor DHCP.

En el paso 104, se descarta el mensaje Discover para impedir que el usuario falsifique la dirección MAC del equipo del lado de la red, por ejemplo falsificando una dirección MAC de un BRAS.

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

En el paso 106, el equipo de acceso reenvía el mensaje DIscover al equipo del lado de la red.

En el paso 107, el equipo del lado de la red devuelve un mensaje “Offer” (Oferta) al equipo de acceso, donde el mensaje Offer transporta 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 el paso 108, el equipo de acceso analiza el mensaje Offer recibido para adquirir una dirección MAC de la fuente del mensaje Offer, es decir, una dirección MAC del equipo del lado de la red.

En el paso 109, el equipo de acceso aprende la dirección MAC del equipo del lado de la red, graba la dirección MAC aprendida del equipo del lado de la red en el equipo de acceso y realiza una operación para impedir que se relocalice una tabla de aprendizaje de direcciones MAC, para impedir que se aprenda la dirección MAC del equipo del lado de la red desde otros puertos.

La operación de impedir que se relocalice la tabla de aprendizaje de direcciones MAC incluye específicamente: generar la tabla de aprendizaje de direcciones MAC utilizando la dirección MAC del equipo del lado de la red, donde la tabla de aprendizaje de direcciones MAC se fija para que sea una tabla estática de direcciones MAC, de manera que la dirección MAC del equipo del lado de la red queda bloqueada para impedir que se elimine la dirección MAC aprendida con el paso del tiempo; y/o configurar un chip lógico para filtrar mensajes que tienen direcciones MAC idénticas a la dirección MAC del equipo del lado de la red y son de otros puertos del lado de usuario, utilizando la dirección MAC aprendida del equipo del lado de la red, por ejemplo, fijando la dirección MAC aprendida del equipo del lado de la red en una tabla de filtrado de direcciones MAC del chip lógico o almacenando la dirección MAC aprendida en el equipo de acceso para proporcionar la petición y filtrado de la dirección MAC.

En el paso 110, el equipo de acceso reenvía el mensaje Offer al UE, donde el mensaje Offer transporta información del equipo del lado de la red.

En el paso 111, el UE envía un mensaje Request (Petición) al equipo de acceso, para solicitar al equipo del lado de la red que asigne una dirección IP para el usuario.

En el paso 112, el equipo de acceso analiza el mensaje Request recibido para adquirir una dirección MAC de la fuente del mensaje Request recibido, es decir, una dirección MAC del UE.

En el paso 113, se juzga si la dirección MAC del UE adquirida por el equipo de acceso es la dirección MAC conocida del equipo del lado de la red. Si la dirección MAC del UE es la dirección MAC conocida del equipo del lado de la red, se efectúa el paso 114; en otro caso, se efectúa el paso 115.

En el paso 114, se descarta el mensaje Request para impedir que el usuario falsifique la dirección MAC del equipo del lado de la red.

En el paso 115, el equipo de acceso aprende la dirección MAC adquirida del UE.

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

En el paso 117, el equipo del lado de la red asigna una dirección IP para el usuario y devuelve un mensaje ACK que transporta la dirección IP asignada para el usuario del equipo de acceso.

En el paso 118, el equipo de acceso analiza el mensaje ACK recibido para adquirir una dirección MAC de la fuente del mensaje ACK, es decir, una dirección MAC del equipo del lado de la red.

En el paso 119, el equipo de acceso aprende la dirección MAC del equipo del lado de la red, graba la dirección MAC aprendida del equipo del lado de la red en el equipo de acceso y efectúa la operación de impedir que la tabla de aprendizaje de direcciones MAC sea reubicada para impedir que aprenda la dirección MAC del equipo del lado de la red de otros puertos.

La operación de impedir que la tabla de aprendizaje de direcciones MAC sea reubicada incluye específicamente: generar la tabla de aprendizaje de direcciones MAC utilizando la dirección MAC del equipo del lado de la red, donde la tabla de aprendizaje de direcciones MAC se fija como una tabla estática de direcciones MAC, de manera que la dirección MAC del equipo del lado de la red queda bloqueada para impedir que la dirección MAC aprendida sea eliminada con el paso del tiempo; y/o configurar el chip lógico para filtrar mensajes que tienen direcciones MAC de la fuente que sean la dirección MAC del equipo del lado de la red y de otros puertos del lado del usuario, utilizando la dirección MAC aprendida del equipo del lado de la red, por ejemplo fijando la dirección MAC aprendida del equipo del lado de la red en una tabla de filtros de direcciones MAC del chip lógico o almacenando la dirección MAC aprendida en el equipo de acceso, para proporcionar la petición y filtrado de la dirección MAC.

En el paso 120, el equipo de acceso reenvía el mensaje ACK al UE, donde el mensaje ACK transporta la dirección IP asignada por el equipo del lado de la red para el usuario.

Si el usuario ha pasado una autentificación de acceso del equipo del lado de la red anteriormente, los pasos 101 a 110 se pueden omitir.

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, de acuerdo con un segundo modo de realización de la presente invención. Un escenario de aplicación de este modo de realización es que un usuario solicite el establecimiento de una sesión empleando la tecnología PPPoE. El proceso principal del método incluye los pasos siguientes.

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

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

En el paso 202, el equipo de acceso recibe el mensaje PADI desde el UE, y analiza el mensaje PADI recibido para adquirir una dirección MAC de la fuente del mensaje PADI recibido, es decir, una dirección MAC del UE.

En el paso 203, se juzga si la dirección MAC del UE adquirida por el equipo de acceso es una dirección MAC conocida por el equipo del lado de la red. Si la dirección MAC del UE es una dirección MAC conocida por el equipo del lado de la red, se efectúa el paso 204; en otro caso, se efectúa el paso 205.

El equipo de acceso puede aprender una dirección MAC del equipo del lado de la red en virtud de un protocolo de encaminamiento u otros métodos. En este modo de realización, el equipo del lado de la red es un BRAS.

En el paso 204, se descarta el mensaje PADI para impedir que el usuario falsifique la dirección MAC del equipo del lado de la red, por ejemplo, falsificando una dirección MAC del BRAS.

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

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

En el paso 207, el equipo del lado de la red devuelve un mensaje de oferta de descubrimiento activo de PPPoE (PADO) al equipo de acceso, donde el mensaje PADO transporta 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 el paso 208, el equipo de acceso analiza el mensaje PADO recibido para adquirir una dirección MAC de la fuente del mensaje PADO, es decir, una dirección MAC del equipo del lado de la red.

En el paso 209, el equipo de acceso aprende la dirección MAC del equipo del lado de la red, graba la dirección MAC aprendida del equipo del lado de la red en el equipo de acceso, y efectúa una operación para impedir que la tabla de aprendizaje de direcciones MAC sea reubicada, de manera que se impida que la dirección MAC del equipo del lado de la red sea aprendida desde otros puertos.

Por ejemplo, se puede generar una tabla estática de aprendizaje de direcciones MAC, o se puede configurar un chip lógico de forma que el chip lógico filtre mensajes que tienen direcciones MAC de la fuente idénticas a las direcciones MAC del equipo del lado de la red y son de otros puertos, utilizando la dirección MAC aprendida del equipo del lado de la red o de la tabla de direcciones MAC generada.

En el paso 210, el equipo de acceso reenvía el mensaje PADO al UE, donde el mensaje PADO transporta información del equipo del lado de la red.

En el paso 211, el UE envía un mensaje de petición de descubrimiento activo de PPPoE (PADR) al equipo de acceso para solicitar los servicios de establecimiento de la sesión.

En el paso 212, el equipo de acceso analiza el mensaje PADR recibido para adquirir una dirección MAC de la fuente del mensaje PADR recibido, es decir, una dirección MAC del UE.

En el paso 213, se juzga si la dirección MAC del 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 efectúa el paso 214; en otro caso, se efectúa el paso 215.

En el paso 214, se descarta el mensaje PADR para impedir que el usuario falsifique la dirección MAC del equipo del lado de la red.

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

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

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

En el paso 218, el equipo de acceso analiza el mensaje PADS recibido para adquirir una dirección MAC de la fuente del mensaje PADS, es decir, una dirección MAC del equipo del lado de la red.

En el paso 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 efectúa la operación de impedir que la tabla de aprendizaje de direcciones MAC sea reubicada para impedir que otros puertos aprendan la dirección MAC del equipo del lado de la red.

Por ejemplo, la tabla de aprendizaje de direcciones MAC puede fijarse como una tabla estática de direcciones MAC, de manera que la dirección MAC del equipo del lado de la red se bloquea para impedir que la dirección MAC aprendida del equipo del lado de la red sea eliminada con el paso del tiempo; y/o se configura un chip lógico para filtrar mensajes que tienen direcciones MAC de la fuente idénticas a la dirección MAC del equipo del lado de la red y son de otros puertos del lado de 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 el paso 220, el equipo de acceso reenvía el mensaje PADS al usuario.

La figura 3 es una vista estructural de un dispositivo para impedir que se falsifique una dirección MAC del lado de la red, de acuerdo con un modo de realización de la presente invención.

El dispositivo incluye una unidad 31 de adquisición, una unidad 32 de juicio, una unidad 33 de aprendizaje y puede incluir además una unidad 34 de fijación, una unidad 35 de almacenamiento, una unidad 36 de generación de tablas de direcciones y una unidad 37 de filtrado.

La unidad 31 de adquisición está adaptada para adquirir y almacenar una dirección MAC de un UE. La unidad 35 de almacenamiento está adaptada para almacenar una dirección MAC adquirida del equipo del lado de la red. La unidad 32 de juicio está adaptada para juzgar si la dirección MAC del UE adquirida por la unidad 31 de adquisición es la dirección MAC del equipo del lado de la red almacenada en la unidad 35 de almacenamiento. La unidad 33 de aprendizaje está adaptada para aprender la dirección MAC del UE y la dirección MAC del equipo del lado de la red, cuando el resultado del juicio de la unidad 32 de juicio es que la dirección MAC del UE no es la dirección MAC del equipo del lado de la red. Específicamente, la dirección MAC del equipo del lado de la red puede ser aprendida en al menos una de las maneras siguientes: adquirir la dirección MAC del equipo del lado de la red mediante un protocolo de encaminamiento; adquirir la dirección MAC del equipo del lado de la red por un ARP; y adquirir 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 36 de generación de tablas de direcciones está adaptada para generar una tabla de aprendizaje de direcciones MAC utilizando la dirección MAC aprendida por la unidad 33 de aprendizaje. La unidad 34 de fijación está adaptada para fijar la tabla de aprendizaje de direcciones MAC de manera que sea una tabla estática de direcciones MAC, para impedir que la tabla de aprendizaje de direcciones MAC generada por la unidad 33 de aprendizaje sea reubicada. La unidad 34 de fijación puede configurar también la dirección MAC aprendida del lado de la red en la unidad 37 de filtrado. La unidad 37 de filtrado efectúa una función de filtrado de direcciones MAC de la fuente por medio de un chip lógico. El chip lógico de la unidad 37 de filtrado graba la tabla de filtrado de direcciones MAC y puede ser configurado para filtrar mensajes que tengan direcciones MAC de la fuente que sean la dirección MAC del equipo del lado de la red y desde otros puertos del lado de usuario, utilizando la tabla de filtrado de direcciones MAC. O, por ejemplo, la unidad 37 de filtrado puede tener una función de motor que obtenga mediante solicitud la dirección MAC del equipo del lado de la red desde la tabla de aprendizaje de direcciones MAC para ser filtrada. La unidad 36 de generación de tablas de direcciones puede ser configurada para fijar directamente un atributo de la tabla de aprendizaje de direcciones MAC para que sea estática durante la generación de la tabla de aprendizaje de direcciones MAC, de acuerdo con la dirección MAC aprendida del equipo de red.

Haciendo referencia a las figuras 1, 2 y 3, el sistema de comunicaciones proporcionado en los modos de realización de la presente invención incluye el equipo de acceso, el 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 que acceda el usuario a la red para que pueda adquirir servicios de red. El UE está principalmente adaptado para proporcionar una función de cliente de acceso de usuario. El equipo del lado de la red está principalmente adaptado para proporcionar información relevante de los servicios de red.

El equipo de acceso, por ejemplo, el DSLAM, proporciona un puerto del lado de usuario y un puerto del lado de la red. El puerto del lado de usuario está adaptado para conectar el 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 básica. El equipo de acceso tiene tablas de direcciones almacenada en él que incluye una tabla estática de direcciones y una tabla dinámica de direcciones. La tabla estática de direcciones está configurada generalmente en el equipo de manera manual y se caracteriza porque la tabla se almacena en el equipo desde el principio una vez que está configurada y no es eliminada con el paso del tiempo. La tabla dinámica de direcciones es generada generalmente por el equipo por medio del aprendizaje automático y se caracteriza porque la tabla se elimina automáticamente después de ser almacenada en el equipo durante un periodo de tiempo. De acuerdo con los modos de realización de la presente invención, el equipo de acceso puede generar la tabla estática de direcciones MAC de acuerdo con la dirección MAC del lado de la red aprendida, para impedir que la tabla de aprendizaje de direcciones MAC sea reubicada, y/o el equipo de acceso puede ser configurado para filtrar mensajes que tienen direcciones MAC de la fuente que son la dirección MAC del equipo del lado de la red, y desde otros puertos del lado de 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 siguientes: adquirir la dirección MAC del equipo del lado de la red por medio de un protocolo de encaminamiento; adquirir la dirección MAC del equipo del lado de la red por medio de un ARP; y recibir un mensaje de respuesta del equipo del lado de la red y adquirir la dirección MAC del equipo del lado de la red.

El equipo del lado de la red es, por ejemplo, el servidor DHCP ilustrado en la figura 1 y el BRAS ilustrado en la figura 2. Como se ilustra en la figura 1, se emplea el modo servidor/cliente entre el servidor DHCP y el UE, en el cual un cliente aplica a un servidor una aplicación de configuración que incluye una dirección IP asignada, una máscara de sub-red, una pasarela predeterminada y otros parámetros, y el servidor devuelve la correspondiente información de configuración que incluye la dirección IP asignada, la máscara de la sub-red, la pasarela predeterminada y otros parámetros, de acuerdo con las políticas. Con el método y dispositivo anteriores para impedir automáticamente que se falsifique la dirección MAC del lado de la red, proporcionados en los modos de realización de la presente invención, solamente cuando la dirección MAC del UE no es la dirección MAC del equipo del lado de la red, se permite al equipo de acceso aprender las direcciones MAC del UE y del equipo del lado de la red para impedir que se reubique la tabla de aprendizaje de direcciones MAC, impidiendo con ello que el usuario falsifique el equipo del

lado de la red para acceder a la red, impidiendo que se aprenda la dirección MAC del equipo del lado de la red desde otros puertos para falsificar la dirección MAC del lado de la red, y siendo más conveniente para la administración y mantenimiento.

Se ha introducido en lo que antecede un método y un dispositivo para impedir que se falsifique la dirección MAC del lado de la red, proporcionados en la presente invención. Se han aplicado aquí ejemplos específicos para elaborar los principios e implementación de la presente invención, pero la ilustración de los modos de realización anteriores pretende meramente ayudar a comprender los esquemas técnicos divulgados en la presente invención. Al mismo tiempo, es evidente para los expertos normales en la técnica que se pueden hacer cambios a la implementación específica y al ámbito de aplicación de la presente invención, basándose en el concepto de la invención. En vista de lo anterior, el contenido de esta memoria no se considerará una limitación de la presente invención.

REIVINDICACIONES

1. Un método para impedir que se falsifique una dirección de control de acceso al medio, MAC, en el lado de la red, que comprende:

recibir en el puerto del lado del usuario de un equipo de acceso, un mensaje de descubrimiento desde un equipo de usuario, UE (101) y analizar el mensaje de descubrimiento del UE para obtener una dirección MAC del UE (102); caracterizado porque el método comprende además:

aprender, por el equipo de acceso, la dirección MAC del UE si la dirección MAC del UE es diferente de la dirección MAC conocida del equipo del lado de la red (105);

reenviar, por el equipo de acceso, el mensaje de descubrimiento al equipo del lado de la red;

recibir, por el equipo de acceso, un mensaje de oferta desde el equipo del lado de la red;

analizar, por el equipo de acceso, un mensaje de oferta para adquirir una dirección MAC del equipo del lado de la red;

aprender, por el equipo de acceso, la dirección MAC del equipo del lado de la red (109);

generar, por el equipo de acceso, una tabla de aprendizaje de direcciones MAC utilizando la dirección MAC aprendida del equipo del lado de la red y fijar la tabla de aprendizaje de direcciones MAC para que sea una tabla estática de direcciones, donde la dirección MAC del equipo del lado de la red en la tabla estática de direcciones queda enclavada; y

filtrar, por el equipo de acceso, mensajes que tienen direcciones MAC de la fuente idénticas a la dirección MAC del equipo del lado de la red y son de otros puertos del lado de usuario del equipo de acceso, utilizando la dirección MAC aprendida del equipo del lado de la red.

2. El método según la reivindicación 1, en el que el aprendizaje de la dirección MAC del equipo del lado de la red comprende:

adquirir la dirección MAC del equipo del lado de la red en virtud de un protocolo de encaminamiento; o

adquirir la dirección MAC del equipo del lado de la red en virtud de un protocolo de resolución de direcciones; o

recibir un mensaje de respuesta del equipo del lado de la red y adquirir la dirección MAC del equipo del lado de la red.

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

descartar el mensaje de descubrimiento del UE si la dirección MAC del UE es la misma que la dirección MAC conocida del equipo del lado de la red.

4. Un dispositivo para impedir que se falsifique una dirección de control de acceso al medio, MAC, del lado de la red, comprende:

una unidad (31) de adquisición, adaptada para recibir un mensaje de descubrimiento desde un equipo de usuario, UE, a través de un puerto del lado de usuario en el dispositivo, y analizar el mensaje de descubrimiento del UE para obtener una dirección MAC del UE;

caracterizada porque el dispositivo comprende además:

una unidad (32) de juicio, adaptada para juzgar si la dirección MAC del UE adquirida por la unidad (31) de adquisición es una dirección MAC conocida de un equipo del lado de la red; y

una unidad (33) de aprendizaje, adaptada para aprender la dirección MAC del UE cuando el resultado del juicio de la unidad (32) de juicio es que la dirección MAC del UE no es la dirección MAC conocida del equipo del lado de la red;

donde el dispositivo está adaptado además para reenviar el mensaje de descubrimiento al equipo del lado de la red, y recibir un mensaje de oferta desde el equipo del lado de la red; donde la unidad (33) de aprendizaje está adaptada además para adquirir una dirección MAC del equipo del lado de la red desde el mensaje de oferta;

donde el dispositivo comprende además: una unidad (36) de generación de tablas de direcciones y una unidad (37) de filtrado, y donde

la unidad (36) de generación de tablas 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, siendo fijada la tabla de aprendizaje de direcciones MAC para que sea una tabla estática de direcciones, donde la dirección MAC del equipo del lado de la red de la tabla estática de direcciones queda enclavada;

la unidad (37) de filtrado está adaptada para filtrar mensajes con direcciones MAC de la fuente que sean la dirección MAC del equipo del lado de la red y de otros puertos del lado de usuario del dispositivo, utilizando la dirección MAC aprendida del equipo del lado de la red.

5. El dispositivo según la reivindicación 4, que comprende además:

una unidad de fijación, adaptada para fijar la tabla de aprendizaje de direcciones MAC generada por la unidad de generación de tablas de direcciones para que sea una tabla estática de direcciones MAC y/o adaptada para configurar la unidad de filtrado.

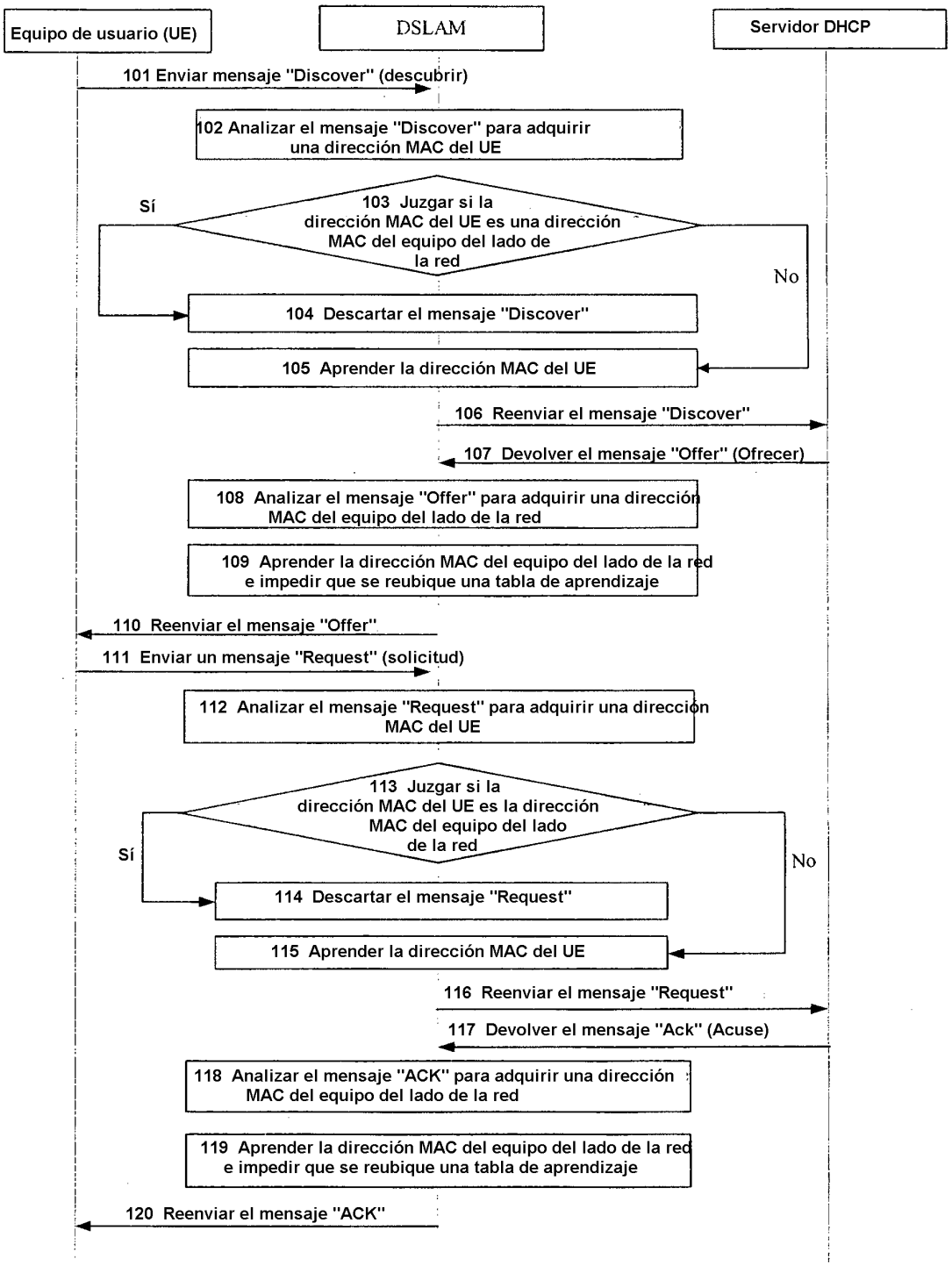
Equipo de usuario (UE)
DSLAM
Servidor DHCP
101 Enviar mensaje "Discover" (descubrir)
102 Analizar el mensaje "Discover" para adquirir una dirección MAC del UE
Sí
103 Juzgar si la dirección MAC del UE es una dirección MAC del equipo del lado de la red
No
104 Descartar el mensaje "Discover"
105 Aprender la dirección MAC del UE
106 Reenviar el mensaje "Discover"
107 Devolver el mensaje "Offer" (Ofrecer)
108 Analizar el mensaje "Offer" para adquirir una dirección MAC del equipo del lado de la red
109 Aprender la dirección MAC del equipo del lado de la red e impedir que se reubique una tabla de aprendizaje
110 Reenviar el mensaje "Offer"
111 Enviar un mensaje "Request" (solicitud)
112 Analizar el mensaje "Request" para adquirir una dirección MAC del UE
113 Juzgar si la dirección MAC del UE es la dirección MAC del equipo del lado de la red
Sí
No
114 Descartar el mensaje "Request"
115 Aprender la dirección MAC del UE
116 Reenviar el mensaje "Request"
117 Devolver el mensaje "Ack" (Acuse)
118 Analizar el mensaje "ACK" para adquirir una dirección MAC del equipo del lado de la red
119 Aprender la dirección MAC del equipo del lado de la red e impedir que se reubique una tabla de aprendizaje
120 Reenviar el mensaje "ACK"

FIG. 1

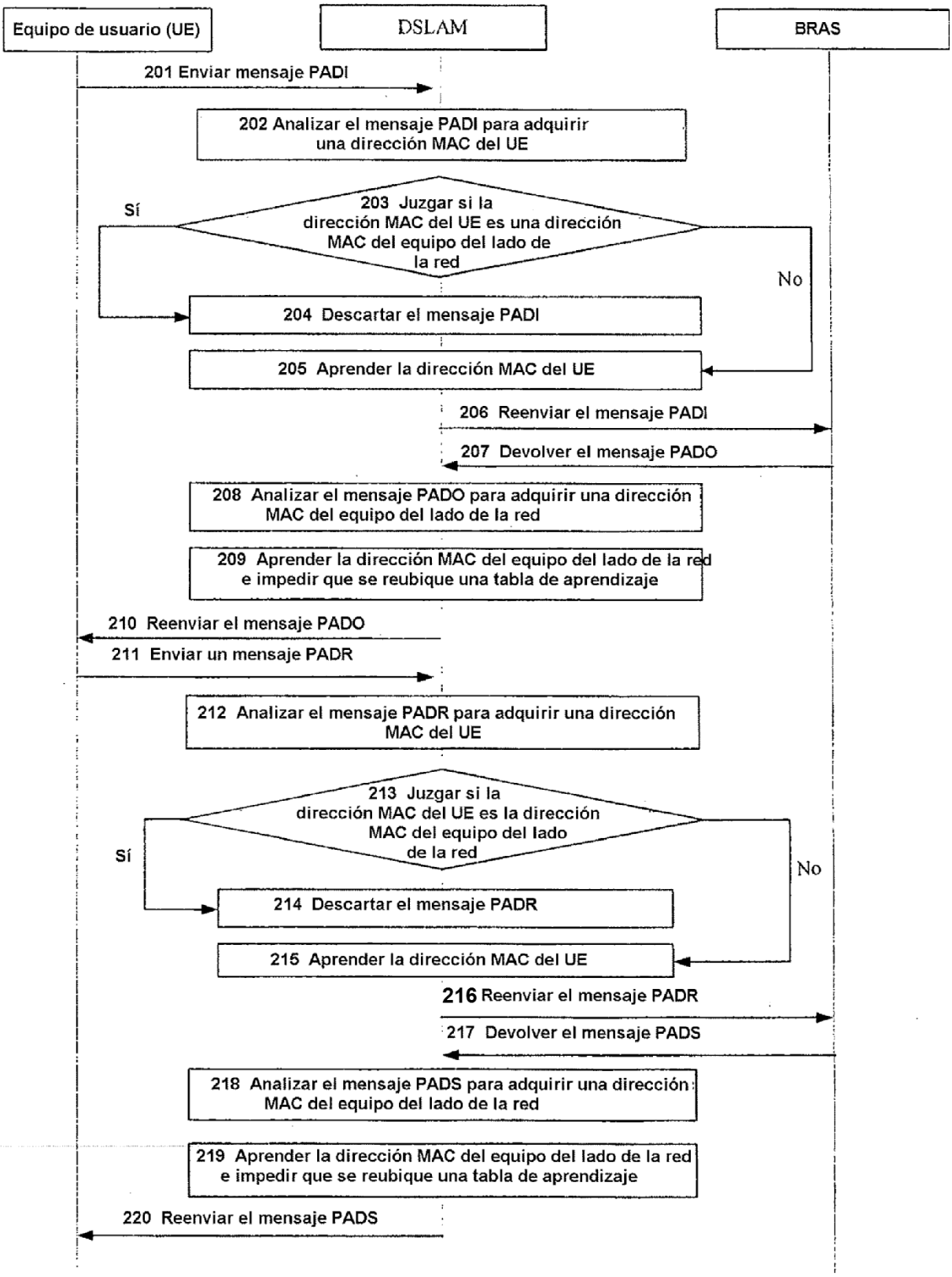
Equipo de usuario (UE)
DSLAM
BRAS
201 Enviar mensaje PADI
202 Analizar el mensaje PADI para adquirir una dirección MAC del UE
Sí
203 Juzgar si la dirección MAC del UE es una dirección MAC del equipo del lado de la red
No
204 Descartar el mensaje PADI
205 Aprender la dirección MAC del UE
206 Reenviar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

FIG. 2

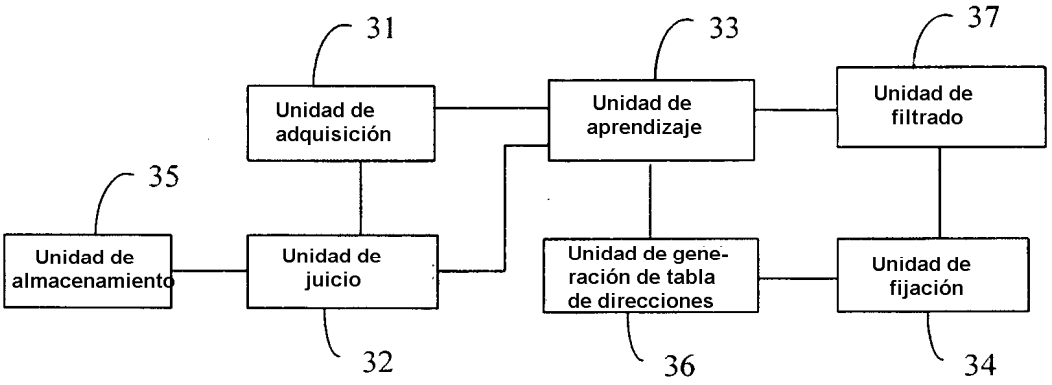
31
33
37
Unidad de adquisición
Unidad de aprendizaje
Unidad de filtrado
35
Unidad de almacenamiento
Unidad de juicio
Unidad de generación de tabla de direcciones
Unidad de fijación
32
36
34

FIG. 3