(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 315**

(51) Int. CI.:
H04L 12/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06722401 .4**
(96) Fecha de presentación: **25.04.2006**
(97) Número de publicación de la solicitud: **1863217**
(97) Fecha de publicación de la solicitud: **05.12.2007**

(54) Título: **Un método, sistema y aparato para impedir la falsificación de una dirección MAC**

(30) Prioridad:
25.04.2005 CN 200510066236

(45) Fecha de publicación de la mención BOPI:
20.09.2012

(45) Fecha de la publicación del folleto de la patente:
20.09.2012

(73) Titular/es:
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI ADMINISTRATION BUILDING, BANTIAN LONGGANG DISTRICT
SHENZHEN GUANGDONG 518129, CN

(72) Inventor/es:
WU, Haijun y
ZHANG, Jun

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Un método, sistema y aparato para impedir la falsificación de una dirección MAC

CAMPO DE LA INVENCIÓN

La presente invención se refiere a las comunicaciones de redes y en particular, a un método, sistema y aparato para impedir la falsificación de dirección de Control de Acceso al Medio.

ANTECEDENTES DE LA INVENCIÓN

Actualmente, dispositivos de acceso tales como Multiplexor de Acceso a la Línea Digital de Abonado (DSLAM) y un Dispositivo de Acceso Integrado se han aplicado, en gran medida, para proporcionar acceso de banda ancha. Dichos dispositivos de acceso pueden proporcionar una diversidad de accesos de banda ancha tales como Bucle de Abonado Digital Asimétrico (ADSL), Línea de Abonado Digital de Alta Tasa de Transferencia de Línea Única (SHDSL), Bucle de Abonado Digital de muy Alta Tasa de Transferencia (VDSL), etc., para permitir a los usuarios acceder a Internet de banda ancha de acceso y para realizar otros servicios tales como servicios de vídeo y servicios de telefonía de IP (Protocolo de Internet).

Actualmente, con el fin de poner en práctica la autenticación y facturación para usuarios y para evitar un acceso malintencionado de usuarios ilícitos, se emplean criterios de filtro basados en la dirección de Control de Acceso al Medio (MAC) para filtrar a los usuarios que acceden a la red.

Sin embargo, con el aumento de los usuarios de banda ancha, algunos usuarios ilícitos acceden ilegalmente a la red de banda ancha por medio de la falsificación de direcciones MAC legales y pueden prestar sus servicios ilícitos o interferir, de forma malintencionada, con los servicios normales en la red de banda ancha. Por ejemplo, algunos usuarios ilícitos pueden cambiar las direcciones MAC de los usuarios legales utilizando herramientas de software para atacar a los usuarios legales e interferir con los servicios de banda ancha normales. Por lo tanto, la red de acceso de banda ancha necesita capacidades para impedir la falsificación de dirección MAC.

Una solución para evitar la falsificación de dirección MAC está vinculada a una dirección MAC fuente con un puerto de origen. Según esta solución, a cada usuario que tiene acceso a la red se le asigna una o más direcciones MAC fuente y se memoriza una relación entre una dirección MAC fuente y un puerto de acceso. De este modo, a la recepción de un paquete de Ethernet enviado desde un usuario a través de un puerto de acceso, un dispositivo de acceso determina si la dirección MAC fuente del paquete coincide con el puerto de acceso. Si la dirección MAC fuente del paquete coincide con el puerto de acceso, el dispositivo de acceso reenvía el paquete a una capa superior de la red de banda ancha; de no ser así, el dispositivo de acceso desecha el paquete. Según esta solución, a cada uno de los puertos de acceso necesita asignarse al menos una dirección MAC fuente correspondiente y esta operación se realiza de forma aleatoria. Cuando existe un gran número de puertos de acceso en la red de banda ancha, la carga de trabajo para proporcionar una o más direcciones MAC fuente para cada uno de los puertos de acceso es bastante pesada. Además, puesto que la dirección MAC fuente está vinculada con el puerto de acceso, si el usuario tiene un nuevo PC o desea cambiar la dirección MAC actual a otra dirección MAC legal, el usuario ha de efectuar la reposición de la dirección MAC fuente en el dispositivo de acceso para prestar servicios, lo que resulta bastante complejo y por ello, esta solución es difícil de aplicarse ampliamente.

El documento US 6.115.376 da a conocer un método para mejorar la seguridad de la red en una red. A la recepción de un paquete en un puerto particular, el proceso implica determinar si el paquete soporta una dirección fuente con la que los datos de autenticación establecen una correspondencia, o mapeo, con el puerto particular. Si el paquete soporta una dirección fuente con la que los datos de autenticación establecen una correspondencia con el puerto particular, en tal caso, se acepta el paquete y en caso contrario, se ejecuta un protocolo de autenticación en el puerto para determinar si la dirección tiene su origen, o no, en un emisor autorizado.

SUMARIO DE LA INVENCIÓN

Un método, un sistema y un aparato para impedir la falsificación de dirección MAC se dan a conocer por las formas de realización de esta invención, con el fin de evitar la falsificación de la dirección MAC y aligerar la carga de trabajo del sistema sin asignar una o más direcciones MAC a cada puerto de acceso.

Un método para impedir la falsificación de dirección MAC comprende:

recibir, por un dispositivo de autenticación, una dirección MAC fuente e información de puerto de acceso de un puerto de acceso desde un dispositivo de acceso, en donde la dirección MAC fuente y la información de puerto de acceso están asociadas con una demanda de autenticación desde el puerto de acceso recibida por el dispositivo de acceso;

determinar, por el dispositivo de autenticación, si la dirección MAC fuente recibida es una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida y

si la dirección MAC fuente recibida es una dirección MAC falsificada, rechazar, por el dispositivo de autenticación, la demanda de autenticación.

La recepción, por el dispositivo de autenticación, de la dirección MAC fuente y de la información de puerto de acceso del puerto de acceso comprende:

añadir por un dispositivo de acceso, la información de puerto de acceso a la demanda de autenticación después de recibir la demanda de autenticación que soporta la dirección MAC fuente desde el puerto de acceso y

recibir, por el dispositivo de autenticación, la demanda de autenticación que soporta la dirección MAC fuente y la información de puerto de acceso desde el dispositivo de acceso.

En otra forma de realización, la recepción, por el dispositivo de autenticación, de la dirección MAC fuente y de la información de puerto de acceso del puerto de acceso comprende:

recibir, por el dispositivo de autenticación, la demanda de autenticación que soporta la dirección MAC fuente desde un dispositivo de acceso que recibe la demanda de autenticación que soporta la dirección MAC fuente desde el puerto de acceso;

enviar un mensaje de interrogación que soporta la dirección MAC fuente al dispositivo de acceso para consultar la información de puerto de acceso del puerto de acceso y

recibir la información de puerto de acceso desde el dispositivo de acceso.

El rechazo de la demanda de autenticación comprende:

el envío, por el dispositivo de autenticación, al dispositivo de acceso de un mensaje que indica que una autenticación correspondiente a la demanda de autenticación es fallida e incluyendo la información de puerto de acceso del puerto de acceso que envía la demanda de autenticación.

La determinación de si la dirección MAC fuente recibida es una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y que corresponde a la dirección MAC fuente recibida, comprende:

determinar, por el dispositivo de autenticación, si la dirección MAC fuente recibida ha sido memorizada, o no, en el dispositivo de autenticación;

si la dirección MAC fuente recibida no se memoriza en el dispositivo de autenticación, la determinación, por el dispositivo de autenticación, de que la dirección MAC fuente recibida no es una dirección MAC falsificada y la memorización de una relación entre la dirección MAC fuente y la información de puerto de acceso recibida;

si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación, la determinación, por el dispositivo de autenticación, de si la información de puerto de acceso recibida es coherente, o no, con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida; si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, la determinación de que la dirección MAC fuente recibida no es una dirección MAC falsificada; si la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, la determinación de que la dirección MAC fuente es una dirección MAC falsificada.

El método puede comprender, además:

el registro, por el dispositivo de autenticación, del número de fallos de autenticación que se producen en el puerto de acceso y la notificación al dispositivo de acceso del cierre del puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido.

El método puede comprender, además:

después de recibir la información de puerto de acceso del puerto de acceso, el registro, por el dispositivo de acceso, del número de los fallos de autenticación que se producen en el puerto de acceso y el cierre del puerto de acceso si el

número de fallos de autenticación, que se producen en el puerto de acceso dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido.

El método puede comprender, además:

memorizar, por el dispositivo de acceso, una relación entre la información MAC fuente y la información de puerto de acceso.

El método puede comprender, además:

la supresión, por el dispositivo de acceso, de la información MAC fuente correspondiente a la información de puerto de acceso recibida, que se memoriza en el propio dispositivo de acceso después de recibir la información de puerto de acceso del puerto de acceso, en donde ocurre un fallo de autenticación.

Un sistema para impedir la falsificación de la dirección MAC, comprende:

un dispositivo de acceso, configurado para recibir una demanda de autenticación desde un puerto de acceso y para enviar una dirección MAC fuente e información de puerto de acceso asociada con la demanda de autenticación y

un dispositivo de autenticación, configurado para recibir la dirección MAC fuente y la información de puerto de acceso asociada con la demanda de autenticación desde el dispositivo de acceso, para determinar si la dirección MAC fuente recibida es una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida y si la dirección MAC fuente recibida es una dirección MAC falsificada, para rechazar la demanda de autenticación.

El dispositivo de autenticación puede comprender:

un módulo identificador de falsificación de dirección MAC, configurado para determinar si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación;

si la dirección MAC fuente recibida no se memoriza en el dispositivo de autenticación, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada y memorizar una relación entre la dirección MAC fuente y la información de puerto de acceso;

si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación, determinar si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida; si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada; si la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, determinar que la dirección MAC fuente es una dirección MAC falsificada.

El dispositivo de acceso puede comprender un primer módulo de conteo, configurado para registrar el número de fallos de autenticación que se producen en el puerto de acceso después de recibir un mensaje que indica que una autenticación correspondiente a la demanda de autenticación es fallida y para cerrar el puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso, satisface una condición.

El dispositivo de autenticación puede comprender:

un segundo módulo de conteo, configurado para registrar el número de fallos de autenticación que se producen en el puerto de acceso y para notificar al dispositivo de acceso el cierre del puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso, satisface una condición.

Un dispositivo de acceso para impedir la falsificación de la dirección MAC puede comprender:

un módulo de acceso, configurado para recibir una demanda de autenticación que soporta una dirección MAC fuente desde un puerto de acceso y para enviar la demanda de autenticación;

un módulo de procesamiento de dirección MAC, configurado para recibir la demanda de autenticación desde el módulo de acceso y para enviar la dirección MAC fuente y la información de puerto de acceso del puerto de acceso, en donde la dirección MAC fuente y la información de puerto de acceso están asociadas con la demanda de autenticación y

un módulo de interfaz de enlace ascendente, configurado para recibir la dirección MAC fuente y la información de puerto de acceso desde el módulo de procesamiento de dirección MAC y para enviar la dirección MAC fuente y la información de puerto de acceso a un dispositivo de autenticación.

El módulo de procesamiento de dirección MAC comprende un módulo de conteo, configurado para registrar el número de fallos de autenticación que se producen en el puerto de acceso después de recibir un mensaje que indica que resultó fallida una autenticación correspondiente a la demanda de autenticación y para cerrar el puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso, satisface una condición.

Un dispositivo de autenticación para impedir la falsificación de dirección MAC comprende:

un módulo de interfaz, configurado para recibir una dirección MAC fuente e información de puerto de acceso de un puerto de acceso, en donde la dirección MAC fuente y la información de puerto de acceso están asociadas con una demanda de autenticación desde un dispositivo de acceso;

un módulo de procesamiento, configurado para determinar si la dirección MAC fuente recibida es una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida y si la dirección MAC fuente recibida es una dirección MAC falsificada, para rechazar la demanda de autenticación.

El módulo de procesamiento comprende:

un módulo de memorización de información de usuario, configurado para memorizar la dirección MAC fuente y la información de puerto de acceso; configurado para determinar si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación;

si la dirección MAC fuente recibida no se memoriza en el dispositivo de autenticación, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada y memorizar una relación entre la dirección MAC fuente y la información de puerto de acceso;

si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación, determinar si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida; si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC recibida, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada; si la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, para enviar un mensaje que indica que la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida;

un módulo identificador de falsificación de dirección MAC, configurado para enviar un mensaje de interrogación que soporta la dirección MAC fuente y la información de puerto de acceso al módulo de memorización de información de usuario; a la recepción del mensaje que indica que la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, para enviar un mensaje de fallo de autenticación al dispositivo de acceso; de no ser así, para enviar la demanda de autenticación a un módulo de autenticación y

el módulo de autenticación, configurado para recibir la demanda de autenticación desde el módulo identificador de falsificación de dirección MAC y para realizar una autenticación.

El módulo identificador de falsificación de dirección MAC comprende:

un módulo de conteo, configurado para registrar el número de fallos de autenticación que se producen en el puerto de acceso y para notificar al dispositivo de acceso el cierre del puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso, satisface una condición. En conformidad con la solución ofrecida por las formas de realización de esta invención, a la recepción de la dirección MAC fuente y de la información de puerto de acceso asociada con una demanda de autenticación, el dispositivo de autenticación determina si la dirección MAC fuente es una dirección MAC falsificada, o no lo es. Si la dirección MAC fuente es una dirección MAC falsificada, el dispositivo de autenticación reenvía al dispositivo de acceso un mensaje de fallo de autenticación. Según esta solución, el dispositivo de acceso no necesita asignar una o más direcciones MAC a cada puerto de acceso, con lo que se libera la carga de trabajo del sistema. Además, aún cuando un usuario cambie un puerto de acceso o una dirección MAC fuente, el dispositivo de acceso no necesita reasignar nuevas direcciones MAC, con lo que se libera la carga de trabajo del sistema y se simplifican las operaciones. Por al menos los motivos anteriores, la solución ofrecida por formas de realización de esta invención se pueden utilizar ampliamente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de flujo de un sistema para impedir la falsificación de dirección MAC según una forma de realización de esta invención;

La Figura 2 es un diagrama esquemático que ilustra un sistema para evitar la falsificación de dirección MAC según una forma de realización de esta invención;

La Figura 3 es un diagrama esquemático que ilustra un dispositivo de acceso para impedir la falsificación de dirección MAC según una forma de realización de esta invención;

La Figura 4 es un diagrama esquemático que ilustra un dispositivo de autenticación para impedir la falsificación de dirección MAC según una forma de realización de esta invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

La presente invención se describirá, a continuación, en detalle haciendo referencia a los dibujos adjuntos y a sus formas de realización.

La Figura 1 representa un diagrama de flujo para impedir la falsificación de dirección MAC según una forma de realización de esta invención. Según se representa en la Figura 1, se pueden incluir varios bloques funcionales.

Bloque 101: Un usuario envía una demanda de autenticación a un dispositivo de acceso por intermedio de un puerto de acceso. La demanda de autenticación soporta una dirección MAC (esto es, una dirección MAC fuente) del puerto de acceso.

Cuando el usuario A, que accede a la red de banda ancha a través del dispositivo de acceso A, inicia un proceso de autenticación, el usuario A envía al dispositivo de acceso A una demanda de autenticación. La demanda de autenticación puede ser un mensaje de Protocolo Punto a Punto sobre Ethernet (PPPOE) o un mensaje de Protocolo de Configuración Dinámica de Hosts (DHCP).

Bloque 102: Después de recibir la demanda de autenticación desde el puerto de acceso, el dispositivo de acceso envía a un dispositivo de autenticación la dirección MAC fuente y la información de puerto de acceso del puerto de acceso relacionada con la demanda de autenticación y memoriza una relación entre la dirección MAC fuente y la información de puerto de acceso del puerto de acceso.

Más concretamente, el dispositivo de acceso puede añadir la información de puerto de acceso en la demanda de autenticación y enviar la demanda de autenticación al dispositivo de autenticación o enviar la información de puerto de acceso al dispositivo de autenticación por intermedio de un protocolo de comunicación especial. Por ejemplo, el dispositivo de acceso envía la demanda de autenticación al dispositivo de autenticación. A la recepción de la demanda de autenticación, si el dispositivo de autenticación detecta que la demanda de autenticación no soporta la información de puerto de acceso, el dispositivo de autenticación envía al dispositivo de acceso un mensaje de interrogación que soporta la dirección MAC fuente. A la recepción del mensaje de interrogación de puerto, el dispositivo de acceso envía al dispositivo de autenticación la información de puerto de acceso correspondiente a la dirección MAC fuente.

El dispositivo de acceso puede añadir también la información de puerto de acceso en un PPPOE o un DHCP o un mensaje de autenticación de PPPOA o convertir el mensaje de PPPOA en el mensaje PPPOE y añadir la información de puerto de acceso en el mensaje PPPOE.

La información de puerto de acceso es información de dirección física del puerto de acceso, tal como información de puerto física del puerto de acceso, información de Red de Área Local Virtual (VLAN) del puerto de acceso, identificador de Canal Virtual/Identificador de Ruta Virtual (VPI/VCI) del puerto de acceso, etc.

Bloque 103: El dispositivo de autenticación recibe la dirección MAC fuente y la información de puerto de acceso asociada con la demanda de autenticación.

Bloque 104: El dispositivo de autenticación determina si la dirección MAC fuente se memoriza en el dispositivo de autenticación. Si la dirección MAC fuente se memoriza en el dispositivo de autenticación, se puede realizar el bloque 106; de no ser así, se puede realizar el bloque 105.

Bloque 105: El dispositivo de autenticación determina que la dirección MAC fuente no es una dirección MAC falsificada y se transmite autenticación y se memoriza una relación de la dirección MAC fuente, la información de puerto de acceso y la información de puerto del dispositivo de autenticación.

Si la dirección MAC fuente no se memoriza en el dispositivo de autenticación, ello indica que la demanda de autenticación se inicia por un nuevo usuario.

Bloque 106: El dispositivo de autenticación recupera la información de puerto de acceso en función de la relación entre la dirección MAC fuente memorizada y la información de puerto de acceso y determina si la información de puerto de acceso enviada por el dispositivo de acceso es coherente, o no, con la información de puerto de acceso recuperada. Si la información de puerto de acceso enviada por el dispositivo de acceso es coherente con la información de puerto de acceso recuperada, el dispositivo de autenticación determina que la dirección MAC fuente es una dirección MAC legal y se transmite la autenticación; de no ser así, se puede realizar el bloque 107.

Si la información de puerto de acceso, en la demanda de autenticación, es coherente con la información de puerto de acceso memoriza en el dispositivo de autenticación, ello indica que la demanda de autenticación se envía por un usuario que ha accedido a la red.

Bloque 107: El dispositivo de autenticación determina que la dirección MAC fuente es una dirección MAC falsificada y reenvía al dispositivo de acceso un mensaje de fallo de autenticación que transmite la información de puerto de acceso.

Además, después de que el dispositivo de acceso determine que la dirección MAC fuente es una dirección MAC falsificada, el número de fallos de autenticación en el puerto de acceso que corresponde a la dirección MAC fuente se registra en el dispositivo de autenticación. Si el número de fallos de autenticación, que se producen en el puerto de acceso dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido, el dispositivo de autenticación notifica al dispositivo de acceso la operación del cierre del puerto de acceso, es decir, para inhibir cualquier información que pretenda entrar en la red a través del puerto de acceso.

Bloque 108: A la recepción del mensaje de fallo de autenticación, el dispositivo de acceso suprime la dirección MAC fuente que se memoriza y corresponde a la información de puerto de acceso soportada en el mensaje de fallo de autenticación.

Además, a la recepción del mensaje de fallo de autenticación, el dispositivo de acceso registra el número de fallos de autenticación que se producen en el puerto de acceso. Si el número de fallos de autenticación que se producen en el puerto de acceso, dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido, el dispositivo de acceso cierra el puerto de acceso.

La Figura 2 representa un diagrama esquemático que ilustra un sistema para impedir la falsificación de dirección MAC según una forma de realización de la presente invención. Según se indica en la Figura 2, el sistema puede incluir un dispositivo de acceso 21 y un dispositivo de autenticación 22.

Un dispositivo de acceso 21 está configurado para recibir una demanda de autenticación que soporta una dirección MAC fuente que se envía por un usuario por intermedio de un puerto de acceso, para enviar al dispositivo de autenticación 22 la dirección MAC fuente y la información de puerto de acceso asociada con la demanda de autenticación y para memorizar una relación entre la dirección MAC fuente y la información de puerto de acceso. A la recepción de un mensaje de fallo de autenticación, que soporta la información de puerto de acceso y se envía por el dispositivo de autenticación 22, el dispositivo de acceso 21 está configurado para suprimir la dirección MAC fuente memorizada correspondiente a la información del puerto de acceso.

El dispositivo de acceso 21 puede incluir un primer módulo de conteo configurado para recibir un mensaje de fallo de autenticación que soporta la información de puerto de acceso y se envía por el dispositivo de autenticación 22, para registrar el número de fallos de autenticación que se producen en el puerto de acceso correspondiente a la información de puerto de acceso y para cerrar el puerto de acceso si el número de fallos de autenticación que se producen en el puerto de acceso dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido.

El dispositivo de acceso puede ser un dispositivo DSLAM que soporta el acceso de banda ancha o un dispositivo de acceso integrado que soporta los accesos de banda ancha y de banda estrecha.

El usuario puede acceder al dispositivo de acceso a través de dichos puertos de acceso como puertos ADSL o SHDSL o VDSL.

El dispositivo de acceso 21 y el dispositivo de autenticación 22 pueden comunicarse entre sí a través de una Red de Área Metropolitana o comunicarse entre sí directamente. El dispositivo de acceso 21 puede conectarse con la Red de Área Metropolitana o con el dispositivo de autenticación 22 a través de su interfaz de Modo de Transferencia Asíncrona (ATM) o la interfaz de Protocolo de Internet (IP).

El dispositivo de autenticación 22 está configurado para recibir la dirección MAC fuente y la información de puerto de acceso asociada con la demanda de autenticación enviada por el dispositivo de acceso 21 y determina si la dirección MAC fuente está memorizada en el dispositivo de autenticación 22. Si la dirección MAC fuente está memorizada en el dispositivo de autenticación 22, dicho dispositivo de autenticación 22 determina si la información de puerto de acceso correspondiente a la dirección MAC fuente memorizada es coherente con la información del puerto de acceso enviada por el dispositivo de acceso 21. Si la información de puerto de acceso correspondiente a la dirección MAC fuente

memorizada no es coherente con la información de puerto de acceso enviada por el dispositivo de acceso 21, el dispositivo de autenticación 22 reenvía al dispositivo de acceso 21 un mensaje de fallo de autenticación que soporta la información de puerto de acceso; de no ser así, el dispositivo de autenticación 22 memoriza una relación de la dirección MAC fuente y la información de puerto de acceso.

El dispositivo de autenticación 22 puede incluir un segundo módulo de conteo configurado para registrar el número de fallos de autenticación que se producen en el puerto de acceso después de que se detecte un fallo de autenticación y para enviar un mensaje de cierre de puerto que soporta la información de puerto de acceso al dispositivo de acceso 21 si el número de fallos de autenticación, que se producen en el puerto de acceso dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido.

El dispositivo de autenticación 22 puede ser un servidor de acceso remoto de banda ancha (BRAS) o un servidor DHCP.

La Figura 3 representa un diagrama esquemático que ilustra una estructura de un dispositivo de acceso para evitar la falsificación de dirección MAC según una forma de realización de esta invención. Según se representa en la Figura 3, el dispositivo de acceso 21 puede incluir un módulo de acceso 211, un módulo de procesamiento de dirección MAC 212 y un módulo de interfaz de enlace ascendente 213.

El módulo de acceso 211 está configurado para recibir una demanda de autenticación que soporta una dirección MAC fuente y se envía por un usuario y para enviar la demanda de autenticación al módulo de procesamiento de dirección MAC 212.

El módulo de acceso 211 está configurado con una interfaz xDSL, que puede ser una interfaz ADSL que incluye ADSL2, ADSL2+, etc., o una interfaz SHDSL o una interfaz VDSL.

El módulo de procesamiento de dirección MAC 212 está configurado para recibir la demanda de autenticación que soporta la dirección MAC fuente desde el módulo de acceso 211, para memorizar una relación entre la dirección MAC fuente y la información de puerto de acceso y para enviar la información de puerto de acceso y la dirección MAC fuente asociada con la demanda de autenticación al módulo de interfaz de enlace ascendente 213. A la recepción de un mensaje de fallo de autenticación, que soporta la información de puerto de acceso enviada desde el módulo de interfaz de enlace ascendente 213, el módulo de procesamiento de dirección MAC 212 suprime la dirección MAC fuente que está memorizada en dicho módulo, en donde la dirección MAC fuente memorizada en el módulo de procesamiento de dirección MAC 212 está vinculada con la información de puerto de acceso soportada en el mensaje de fallo de autenticación.

El módulo de procesamiento de dirección MAC 212 puede incluir un módulo de conteo configurado para recibir un mensaje de fallo de autenticación que soporta la información de puerto de acceso desde el módulo de interfaz de enlace ascendente 213, para registrar el número de fallos de autenticación que se producen en el puerto de acceso correspondiente a la información de puerto de acceso soportada en el mensaje de fallo de autenticación y para cerrar el puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido.

El módulo de interfaz de enlace ascendente 213 está configurado para enviar a un dispositivo de autenticación 22 la dirección MAC fuente y la información de puerto de acceso asociada con la demanda de autenticación desde el módulo de procesamiento de dirección MAC 212 y para enviar al módulo de procesamiento de dirección MAC 212 el mensaje de fallo de autenticación que soporta la información de puerto de acceso recibida desde el dispositivo de autenticación 22.

El módulo de interfaz de enlace ascendente 213 puede estar configurado con dichas interfaces de enlace ascendente tal como interfaz de Ethernet Gigabit (GE) (p.e., interfaz de GE óptica o interfaz de GE eléctrica), interfaz de Fast Ethernet (FE) (p.e., interfaz FE óptica o interfaz FE eléctrica), interfaz de Modo de Transferencia Síncrona (STM) -1 (p.e., interfaz óptica STM-1 o interfaz eléctrica STM-1), la interfaz E1, la interfaz E3 o la interfaz STM-4.

La Figura 4 representa un diagrama esquemático que ilustra una estructura de un dispositivo de autenticación para impedir la falsificación de dirección MAC según una forma de realización de la invención. Según se representa en la Figura 4, el dispositivo de autenticación 22 puede incluir un módulo de memorización de información de usuario 221, un módulo identificador de falsificación de dirección MAC 222 y un módulo de autenticación 223.

El módulo de memorización de información de usuario 221 está configurado para memorizar una relación entre la dirección MAC fuente y la información de puerto de acceso. A la recepción de un mensaje de interrogación que soporta la dirección MAC fuente y la información de puerto de acceso desde el módulo identificador de falsificación de dirección MAC 222, si el módulo de memorización de información de usuario 221 detecta que la dirección MAC fuente, soportada en el mensaje de interrogación, no está memorizada en el módulo de memorización de información de usuario 221, dicho módulo de memorización de información de usuario 221 envía al módulo identificador de falsificación de dirección MAC 222 un mensaje que indica que no existe la dirección MAC fuente y memoriza una relación de la dirección MAC fuente, la información de puerto de acceso y la información de puerto del dispositivo de autenticación. Si el módulo de memorización de información de usuario 221 detecta que la dirección MAC fuente, transmitida en el mensaje de

interrogación, está memorizada en el módulo de memorización de información de usuario 221 y la información de puerto de acceso memorizada, que está vinculada con la dirección MAC fuente, no es coherente con la información de puerto de acceso enviada por el módulo identificador de falsificación de dirección MAC 222, el módulo de memorización de información de usuario 221 reenvía al módulo identificador de falsificación de dirección MAC 222 un mensaje que indica que la información de puerto de acceso desde el módulo identificador de falsificación de dirección MAC 222 no es coherente con la información de puerto de acceso memorizada en el módulo de memorización de información de usuario 221. Si el módulo de memorización de información de usuario 221 detecta que la dirección MAC fuente está memorizada en el módulo de memorización de información de usuario 221 y la información de puerto de acceso memorizada, que está vinculada con la dirección MAC fuente, es coherente con la información de puerto de acceso enviada por el módulo identificador de falsificación de dirección MAC 222, el módulo de memorización de información de usuario 221 reenvía al módulo identificador de falsificación de dirección MAC 222 un mensaje que indica que la información del puerto de acceso desde el módulo identificador de falsificación de dirección MAC 222 es coherente con la información de puerto de acceso memorizada en el módulo de memorización de información de usuario 221.

El módulo identificador de falsificación de dirección MAC 222 está configurado para recibir la dirección MAC fuente y la información de puerto de acceso asociada con la demanda de autenticación desde el dispositivo de acceso 21 y para enviar al módulo de memorización de información de usuario 221 un mensaje de interrogación que soporta la dirección MAC fuente y la información de puerto de acceso. A la recepción del mensaje que indica que la información de dirección MAC fuente no existe o el mensaje que indica que la información de puerto de acceso desde el módulo identificador de falsificación de dirección MAC 222 es coherente con la información de puerto de acceso memorizada en el módulo de memorización de información de usuario 221, el módulo identificador de falsificación de dirección MAC 222 determina que la dirección MAC fuente no es una dirección MAC falsificada y envía la demanda de autenticación al módulo de autenticación 223. A la recepción del mensaje que indica que la información de puerto de acceso desde el módulo identificador de falsificación de dirección MAC 222 no es coherente con la información de puerto de acceso memorizada en el módulo de memorización de información de usuario 221, el módulo identificador de falsificación de dirección MAC 222 reenvía al dispositivo de acceso 21 un mensaje de fallo de autenticación que soporta la información de puerto de acceso que está incluida en el mensaje de interrogación.

El módulo identificador de falsificación de dirección MAC 222 puede incluir un módulo de conteo configurado para contar el número de fallos de autenticación que se producen en el puerto de acceso después de que se detecte un fallo de autenticación y notifica al dispositivo de acceso 21 el cierre del puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso dentro de un periodo de tiempo preestablecido, es mayor que un número preestablecido.

El módulo identificador de falsificación de dirección MAC 222 soporta mensajes de PPPOE, mensajes de PPPOA, mensajes de DHCP, etc.

El módulo de autenticación 223 está configurado para recibir la demanda de autenticación desde el módulo identificador de falsificación de dirección MAC 222 y para realizar una autenticación.

El módulo de autenticación soporta también mensajes PPPOE, mensajes PPPOA, mensajes DHCP, etc.

La descripción anterior de las formas de realización, dadas a conocer en la presente invención, se proporciona para habilitar a los expertos en esta técnica a hacer o utilizar la presente invención. Varias modificaciones a estas formas de realización serán fácilmente evidentes para los expertos en esta materia y los principios genéricos aquí definidos se pueden aplicar a otras formas de realización sin desviarse por ello del alcance de protección de la invención. De este modo, la presente invención no está prevista que esté limitada a las formas de realización aquí descritas si no que admite el más amplio alcance de protección coherente con los principios e ideas inventivas aquí dadas a conocer.

REIVINDICACIONES

1. Un método para impedir la falsificación de una dirección de Control de Acceso al Medio (MAC), caracterizado porque comprende:

recibir, mediante un dispositivo de autenticación, una dirección MAC fuente e información de puerto de acceso de un puerto de acceso desde un dispositivo de acceso, en donde la dirección MAC fuente y la información de puerto de acceso están asociadas con una demanda de autenticación desde el puerto de acceso recibida por el dispositivo de acceso;

determinar, mediante el dispositivo de autenticación, si la dirección MAC fuente recibida es una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida y

si la dirección MAC fuente recibida es una dirección MAC falsificada, rechazar, por el dispositivo de autenticación, la demanda de autenticación.

2. El método según la reivindicación 1, en donde la recepción, por el dispositivo de autenticación, de la dirección MAC fuente y de la información de puerto de acceso del puerto de acceso comprende:

la adición, por un dispositivo de acceso, de información de puerto de acceso a la demanda de autenticación después de recibir la demanda de autenticación que transmite la dirección MAC fuente desde el puerto de acceso y

la recepción, por el dispositivo de autenticación, de la demanda de autenticación que transmite la dirección MAC fuente y de la información de puerto de acceso desde el dispositivo de acceso.

3. El método según la reivindicación 1, en donde la recepción, por el dispositivo de autenticación, de la dirección MAC fuente y de la información de puerto de acceso del puerto de acceso comprende:

la recepción, por el dispositivo de autenticación, de la demanda de autenticación que transmite la dirección MAC fuente desde un dispositivo de acceso que recibe la demanda de autenticación que transmite la dirección MAC fuente desde el puerto de acceso;

el envío de un mensaje de interrogación que transmite la dirección MAC fuente al dispositivo de acceso para demandar la información de puerto de acceso del puerto de acceso y

la recepción de la información de puerto de acceso desde el dispositivo de acceso.

4. El método según la reivindicación 2 o 3, en donde el rechazo de la demanda de autenticación comprende:

el envío, por el dispositivo de autenticación, al dispositivo de acceso de un mensaje que indica un fallo de autenticación correspondiente a la demanda de autenticación e incluye la información de puerto de acceso del puerto de acceso que envía la demanda de autenticación.

5. El método según la reivindicación 1, 2 o 3, en donde la determinación de si la dirección MAC fuente recibida es una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y que corresponde a la dirección MAC fuente recibida comprende:

determinar, por el dispositivo de autenticación, si la dirección MAC fuente recibida ha sido memorizada, o no, en el dispositivo de autenticación;

si la dirección MAC fuente recibida no se memoriza en el dispositivo de autenticación, la determinación, por el dispositivo de autenticación, de que la dirección MAC fuente recibida no es una dirección MAC falsificada y la memorización de una relación entre la dirección MAC fuente y la información de puerto de acceso recibida;

si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación, determinar, por el dispositivo de autenticación, si la información de puerto de acceso recibida es coherente, o no, con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y que corresponde a la dirección MAC fuente recibida; si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, la determinación de que la dirección MAC fuente recibida no es una dirección MAC falsificada; si la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, la determinación de que la dirección MAC fuente es una dirección MAC falsificada.

6. El método según la reivindicación 2 o 3, que comprende, además:

el registro, por el dispositivo de autenticación, del número de fallos de autenticación que ocurren en el puerto de acceso y la notificación al dispositivo de acceso el cierre del puerto de acceso si el número de fallos de autenticación, que ocurren en el puerto de acceso dentro de un periodo de tiempo preestablecido, es superior a un número preestablecido.

7. El método según la reivindicación 4 que comprende, además:

después de recibir la información de puerto de acceso del puerto de acceso, el registro, por el dispositivo de acceso, del número de fallos de autenticación que se producen al nivel del puerto de acceso y el cierre del puerto de acceso si el número de fallos de autenticación, que se producen a nivel del puerto de acceso en un periodo de tiempo preestablecido, es superior a un número preestablecido.

8. El método según cualquiera de las reivindicaciones 2 a 7 que comprende, además:

la memorización, por el dispositivo de acceso, de una relación entre la información MAC fuente y la información de puerto de acceso.

9. El método según la reivindicación 4 o 7, que comprende, además:

la supresión, por el dispositivo de acceso, de la dirección MAC fuente correspondiente a la información de puerto de acceso recibida que se memoriza en el propio dispositivo de acceso después de recibir la información de puerto de acceso del puerto de acceso, en donde ocurre un fallo de autenticación.

10. Un sistema para impedir la falsificación de dirección de Control de Acceso al Medio (MAC) caracterizado porque comprende:

un dispositivo de acceso, configurado para recibir una demanda de autenticación desde un puerto de acceso y para enviar una dirección MAC fuente e información de puerto de acceso asociada con la demanda de autenticación y

un dispositivo de autenticación, configurado para recibir la dirección MAC fuente y la información de puerto de acceso asociada con la demanda de autenticación desde el dispositivo de acceso, para determinar si la dirección MAC fuente recibida es, o no, una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida y si la dirección MAC fuente recibida es una dirección MAC falsificada, rechazar la demanda de autenticación.

11. El sistema según la reivindicación 10, en donde el dispositivo de autenticación comprende:

un módulo identificador de falsificación de dirección MAC, configurado para determinar si la dirección MAC fuente recibida está memorizada, o no, en el dispositivo de autenticación;

si la dirección MAC fuente recibida no está memoriza en el dispositivo de autenticación, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada y memorizar una relación entre la dirección MAC fuente y la información de puerto de acceso;

si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación, determinar si la información de puerto de acceso recibida es coherente, o no, con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida; si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada; si la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, determinar que la dirección MAC fuente es una dirección MAC falsificada.

12. El sistema según la reivindicación 10 o 11, en donde el dispositivo de acceso comprende un primer módulo de conteo, configurado para registrar el número de fallos de autenticación que ocurren en el puerto de acceso después de recibir un mensaje que indica que una autenticación correspondiente a la demanda de autenticación está fallida y para cerrar el puerto de acceso si el número de fallos de autenticación, que ocurren en el puerto de acceso, satisface una condición.

13. El sistema según la reivindicación 10 o 11, en donde el dispositivo de autenticación comprende:

un segundo módulo de conteo, configurado para registrar el número de fallos de autenticación que ocurren en el puerto de acceso y para notificar al dispositivo de acceso el cierre del puerto de acceso si el número de fallos de autenticación, que ocurren en el puerto de acceso, satisface una condición.

14. Un dispositivo de acceso para impedir la falsificación de una dirección de Control de Acceso al Medio (MAC), caracterizado porque comprende:

un módulo de acceso, configurado para recibir una demanda de autenticación que transmite una dirección MAC fuente desde un puerto de acceso y para enviar la demanda de autenticación;

un módulo de procesamiento de dirección MAC, configurado para recibir la demanda de autenticación desde el módulo de acceso y para enviar la dirección MAC fuente y la información de puerto de acceso del puerto de acceso, en donde la dirección MAC fuente y la información de puerto de acceso están asociadas con la demanda de autenticación y

un módulo de interfaz de enlace ascendente, configurado para recibir la dirección MAC fuente y la información e información de puerto de acceso desde el módulo de procesamiento de dirección MAC y para enviar la dirección MAC fuente y la información de puerto de acceso a un dispositivo de autenticación.

15. El dispositivo de acceso según la reivindicación 14, en donde el módulo de procesamiento de dirección MAC comprende un módulo de conteo, configurado para registrar el número de fallos de autenticación que ocurren en el puerto de acceso después de recibir un mensaje que indica que se produjo un fallo en una autenticación correspondiente a la demanda de autenticación y para cerrar el puerto de acceso si el número de fallos de autenticación, que ocurren en el puerto de acceso, satisface una condición.

16. Un dispositivo de autenticación para impedir la falsificación de dirección de Control de Acceso al Medio (MAC) caracterizado porque comprende:

un módulo de interfaz, configurado para recibir una dirección MAC fuente e información de puerto de acceso de un puerto de acceso, en donde la dirección MAC fuente y la información de puerto de acceso están asociadas con una demanda de autenticación desde un dispositivo de acceso;

un módulo de procesamiento, configurado para determinar si la dirección MAC fuente recibida es, o no, una dirección MAC falsificada en función de la dirección MAC fuente recibida, de la información de puerto de acceso recibida y de la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida y si la dirección MAC fuente recibida es una dirección MAC falsificada, rechazar la demanda de autenticación.

17. El dispositivo de autenticación según la reivindicación 16, en donde el módulo de procesamiento comprende:

un módulo de memorización de información de usuario, configurado para memorizar la dirección MAC fuente y la información de puerto de acceso; configurado para determinar si la dirección MAC fuente recibida se memoriza, o no, en el dispositivo de autenticación;

si la dirección MAC fuente recibida no se memoriza en el dispositivo de autenticación, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada y memorizar una relación entre la dirección MAC fuente y la información de puerto de acceso;

si la dirección MAC fuente recibida se memoriza en el dispositivo de autenticación, determinar si la información de puerto de acceso recibida es coherente, o no, con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida;

si la información de puerto de acceso recibida es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, determinar que la dirección MAC fuente recibida no es una dirección MAC falsificada; si la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, para enviar un mensaje que indica que la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida;

un módulo identificador de falsificación de dirección MAC, configurado para enviar un mensaje de interrogación que transmite la dirección MAC fuente y la información de puerto de acceso al módulo de memorización de información de usuario; al recibo del mensaje que indica que la información de puerto de acceso recibida no es coherente con la información de puerto de acceso que se memoriza en el dispositivo de autenticación y corresponde a la dirección MAC fuente recibida, para enviar un mensaje de fallo de autenticación al dispositivo de acceso; de no ser así, para enviar la demanda de autenticación a un módulo de autenticación y

el módulo de autenticación, configurado para recibir la demanda de autenticación desde el módulo identificador de falsificación de dirección MAC y para realizar una autenticación.

18. El dispositivo de autenticación según la reivindicación 17, en donde el módulo identificador de falsificación de dirección MAC comprende:

un módulo de conteo, configurado para registrar el número de fallos de autenticación que se producen en el puerto de acceso y para notificar al dispositivo de acceso el cierre del puerto de acceso si el número de fallos de autenticación, que se producen en el puerto de acceso, satisface una condición.

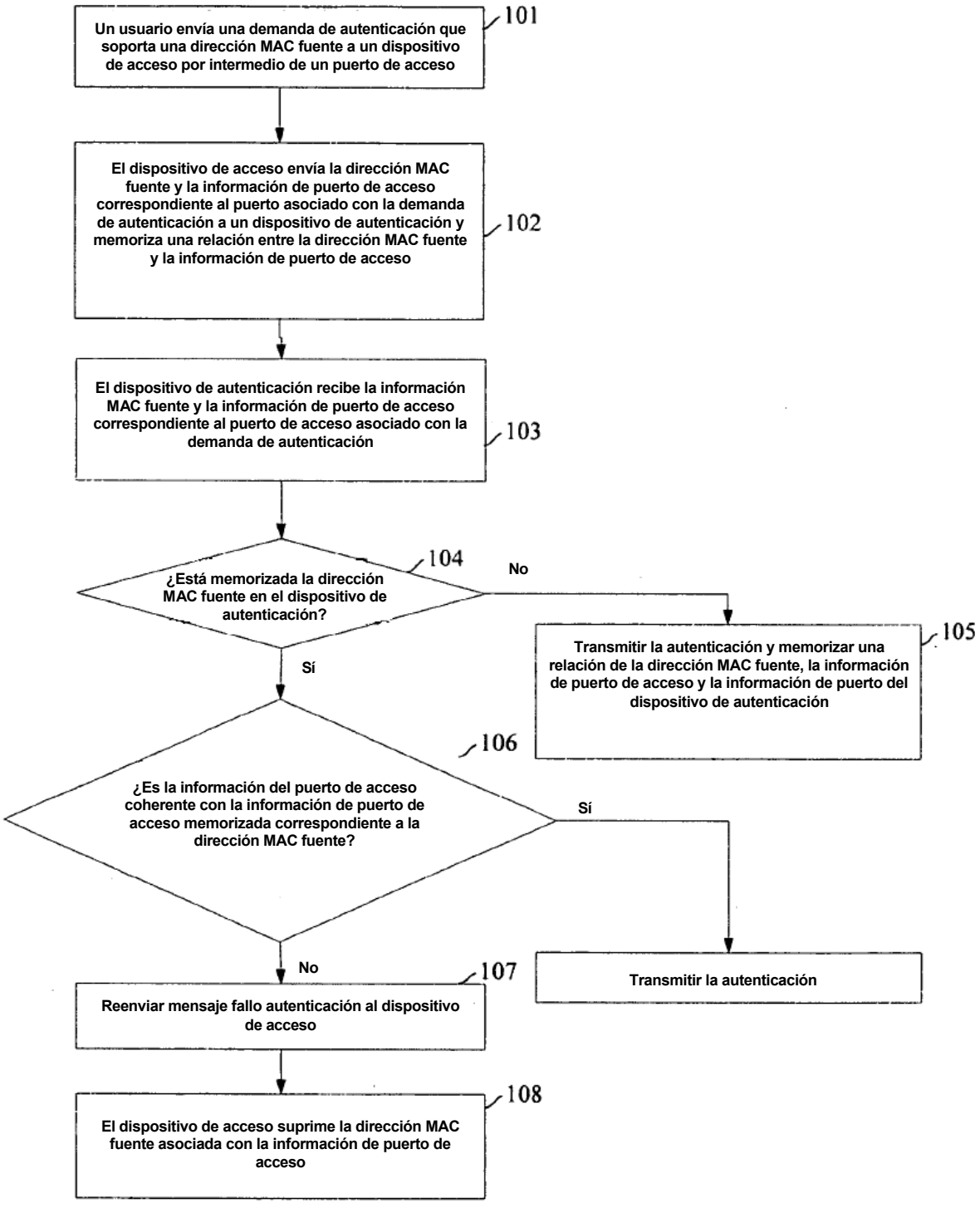
Un usuario envía una demanda de autenticación que soporta una dirección MAC fuente a un dispositivo de acceso por intermedio de un puerto de acceso
101
El dispositivo de acceso envía la dirección MAC fuente y la información de puerto de acceso correspondiente al puerto asociado con la demanda de autenticación a un dispositivo de autenticación y memoriza una relación entre la dirección MAC fuente y la información de puerto de acceso
102
El dispositivo de autenticación recibe la información MAC fuente y la información de puerto de acceso correspondiente al puerto de acceso asociado con la demanda de autenticación
103
¿Está memorizada la dirección MAC fuente en el dispositivo de autenticación?
104
No
Sí
Transmitir la autenticación y memorizar una relación de la dirección MAC fuente, la información de puerto de acceso y la información de puerto del dispositivo de autenticación
105
¿Es la información del puerto de acceso coherente con la información de puerto de acceso memorizada correspondiente a la dirección MAC fuente?
106
Sí
No
Transmitir la autenticación
Reenviar mensaje fallo autenticación al dispositivo de acceso
107
El dispositivo de acceso suprime la dirección MAC fuente asociada con la información de puerto de acceso
108

Figura 1

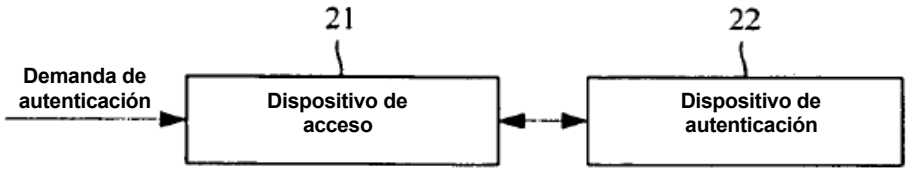

Figura 2

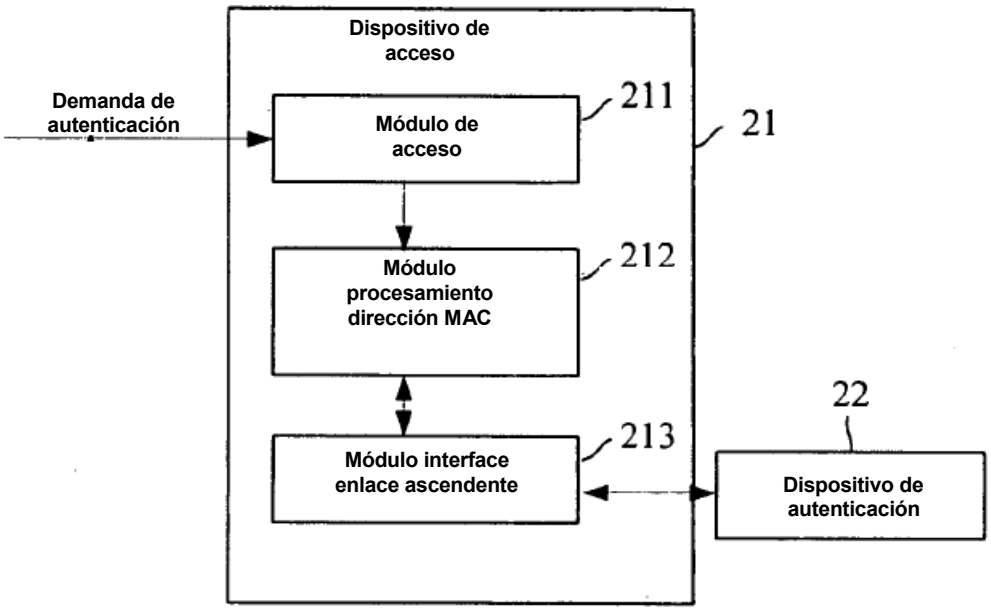

Figura 3

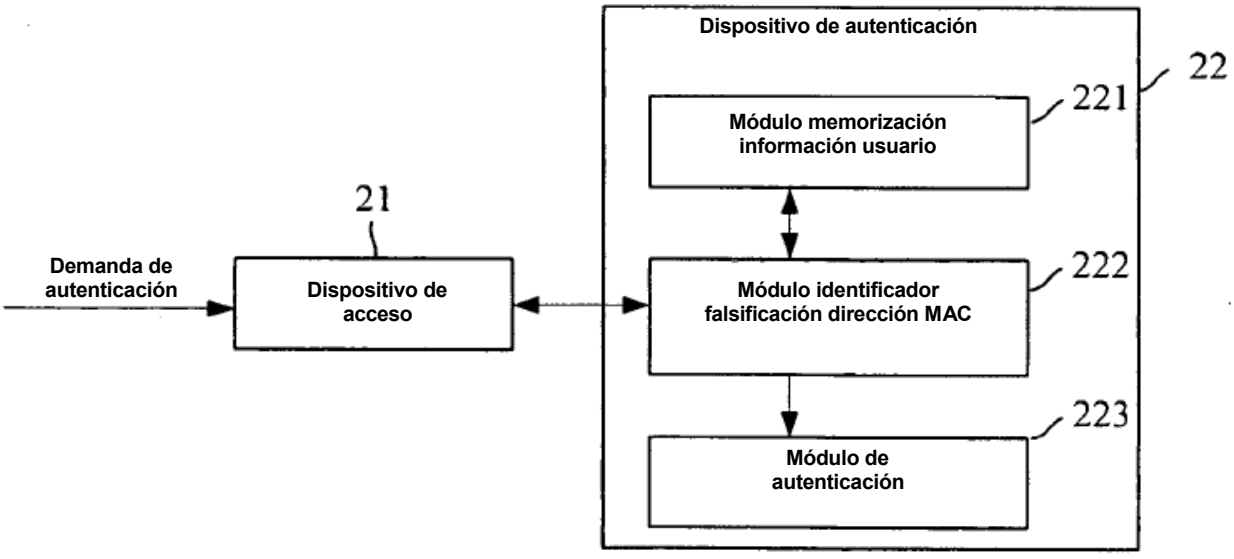

Figura 4