(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 800 913**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/815 (2013.01)
H04W 12/06 (2009.01)
H04W 12/08 (2009.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.08.2016 E 16186714 (8)**

(97) Fecha y número de publicación de la concesión europea: **29.04.2020 EP 3139568**

(54) Título: **Dispositivo de control de acceso y método de control de autenticación**

(30) Prioridad:

02.09.2015 CN 201510556295

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.01.2021

(73) Titular/es:

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

(72) Inventor/es:

HAN, ZHICHONG y
YU, BIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo de control de acceso y método de control de autenticación

Campo técnico

La presente invención se relaciona con el campo de las comunicaciones, y en concreto, con un dispositivo de control de acceso y un método de control de autenticación

Antecedentes

En la comunicación por cable o inalámbrica, cuando un terminal se ha de conectar a una red de área local, el terminal puede necesitar realizar la autenticación de acceso con un servidor de autenticación usando un controlador de acceso. Ya que la capacidad de procesamiento del controlador de acceso es limitada, cuando una cantidad relativamente grande de terminales realizan de manera simultánea la autenticación de acceso, el controlador de acceso se puede sobrecargar.

Para evitar la sobrecarga, el controlador de acceso puede restringir la tasa de paquetes de autenticación recibidos. Por ejemplo, el controlador de acceso preestablece una tasa de paquetes de autenticación recibidos a x, y cuando la tasa total a la que se reciben los paquetes de autenticación de los terminales alcanza x, descarta otro paquete de autenticación que llega en este momento. Se interrumpe un proceso de autenticación de un terminal que envía el paquete de autenticación descartado. El terminal cuyo proceso de autenticación es interrumpido puede reiniciar la autenticación de acceso.

Si los terminales que realizan la autenticación están excesivamente concentrados dentro de un periodo de tiempo, se interrumpen los procesos de autenticación de una gran cantidad de terminales. Los terminales cuyos procesos de autenticación se interrumpen pueden reiniciar de manera inmediata la autenticación, y una tasa de paquetes de autenticación es aún muy grande. La situación en la que una gran cantidad de terminales realizan la autenticación de una manera continua concentrada, y los procesos de interacción de otros terminales se interrumpen. Este proceso se repite de manera continua, provocando finalmente que casi todos los usuarios sean incapaces de completar un proceso de autenticación completo. El fenómeno anterior es llamado un efecto avalancha de autenticación, que afecta a la eficiente de autenticación del sistema.

El documento US 2006/0282880 A1 describe un método para manejar las solicitudes de autenticación en una red, en donde las solicitudes de autenticación pueden tener diferentes tipos, comprendiendo el método las etapas de determinar los tipos de solicitudes de autenticación, y aplicar una política para manejar las solicitudes de autenticación recibidas en base a los tipos determinados de solicitudes de autenticación.

El documento US 2009/0300759 A1 describe tasas limitantes que evitan que el sistema que recibe los paquetes sea abrumado con paquetes que son potencialmente parte de un ataque en el sistema. En una realización de enrutador o conmutador, como resultado de limitar en tasa un puerto para paquetes que coinciden con una ACL, sólo un cierto número de paquetes que coinciden con los paquetes de la ACL son enviados por el enrutador o el conmutador, el exceso de paquetes se descarta. Una vez que se determina que el periodo de la tasa limitante ha expirado, el puerto se abre a plena tasa para que el tráfico coincida con la ACL coincidente.

Compendio

Para resolver un problema de un efecto avalancha de autenticación provocado cuando los terminales realizan autenticación de una manera excesivamente concentrada, esta aplicación proporciona un método de control de autenticación y un dispositivo de control de acceso según las reivindicaciones independientes.

Breve descripción de los dibujos

Para describir las soluciones técnicas en las realizaciones de la presente invención de manera más clara, a continuación, se describe brevemente los dibujos adjuntos requeridos para describir las realizaciones. Aparentemente, los dibujos adjuntos en la siguiente descripción muestran simplemente algunas realizaciones de la presente invención, y una persona de experiencia ordinaria en la técnica puede aún derivar otros dibujos a partir de estos dibujos adjuntos sin grandes esfuerzos creativos.

La FIG. 1 es un diagrama de arquitectura de un entorno de red involucrado en la presente invención;

La FIG. 2 es un diagrama de flujo del método de un método de control de autenticación según una realización de la presente invención;

La FIG. 3A es un diagrama de flujo del método de un método de control de autenticación según otra realización de la presente invención;

La FIG. 3B es un diagrama de flujo de las interacciones de la autenticación EAP según la realización mostrada en la FIG. 3A;

La FIG. 3C es un diagrama de una estructura de encapsulación de un paquete EAP según la realización mostrada en la FIG. 3A;

La FIG. 3D es un diagrama de formato de un cuerpo de paquete de un paquete EAP si un campo de tipo de paquete en el paquete EAP es 0 según la realización mostrada en la FIG. 3A;

La FIG. 3E es un diagrama de formato de un formato de un campo de datos en un cuerpo de paquete mostrado cuando un tipo del cuerpo de paquete es Solicitud o Respuesta según la realización mostrada en la FIG. 3A;

La FIG. 3F es un diagrama de flujo de interacciones de autenticación de portal cautiva según la realización mostrada en la FIG. 3A;

La FIG. 4 es un diagrama estructural de un dispositivo de control de acceso según una realización de la presente invención;

La FIG. 5 es un diagrama estructural de un dispositivo de control de acceso según otra realización de la presente invención; y

La FIG. 6 es un diagrama de bloques de un dispositivo de red según una realización de la presente invención.

Descripción de las realizaciones

Para tener los objetivos, soluciones técnicas y ventajas de la presente invención más claras, a continuación, se describen además las maneras de implementación de la presente invención en detalle con referencia a los dibujos adjuntos.

Referente a la FIG. 1, que muestra un diagrama de la arquitectura de un entorno de red involucrado en la presente invención. La red incluye los siguientes dispositivos de red: un terminal 110, un dispositivo 120 de control de acceso, un servidor 130 de autenticación. Opcionalmente, el entorno de red puede incluir además un servidor 140 de portal (en inglés: portal server).

El dispositivo 120 de control de acceso es un dispositivo de red configurado para procesar un paquete de autenticación entre el terminal 110 y el servidor 130 de autenticación. Por ejemplo, el dispositivo 120 de control de acceso puede ser un controlador de acceso dedicado, o puede ser un dispositivo de red (por ejemplo, un enrutador o un conmutador de red) integrado con una función de un controlador de acceso. El servidor 140 de portal puede ser un ordenador personal, o puede ser un servidor de aplicación web servidora (en inglés: web). El servidor web incluye software para autenticación de portal cautivo (en inglés: captive portal).

El dispositivo 120 de control de acceso se conecta al servidor 130 de autenticación, y el servidor 140 de portal se conecta al dispositivo 120 de control de acceso.

Existen principalmente dos maneras para realizar la autenticación de acceso por el terminal 110. Una es una forma de autenticación de Protocolo de Autenticación Extensible (en inglés: Extensible Authentication Protocol, EAP para abreviar), y la otra es una forma de autenticación de portal cautivo. Al realizar la autenticación de acceso en la forma de autenticación EAP, el terminal 110 se conecta al dispositivo 120 de control de acceso; al realizar la autenticación de acceso en la forma de autenticación de portal cautivo, el terminal 110 se conecta al servidor 140 de portal.

Según una solución mostrada en las realizaciones de la presente invención, se restringe una tasa a la que el dispositivo 120 de control de acceso recibe un paquete de inicio de autenticación (esto es, el primer paquete usado para iniciar un proceso de autenticación) para controlar la cantidad de terminales que entran a un proceso de autenticación posterior por unidad de tiempo, lo que evita un efecto avalancha de autenticación inalámbrica provocado cuando una cantidad excesivamente grande de terminales entran de manera simultánea en la autenticación posterior, y asegura que un terminal que ya realiza la autenticación de acceso posterior actualmente puede completar un proceso de autenticación completo sin problemas.

Cuando no se produce efecto avalancha, puede no restringirse la tasa del paquete de inicio de autenticación. Por lo tanto, para reducir los recursos de procesamiento, en la solución mostrada en las realizaciones de la presente invención, cuando el proceso de autenticación del terminal 110 está siendo controlado, se puede restringir una tasa del paquete de inicio de autenticación sólo cuando se satisface una condición específica.

En un aspecto, se pueden monitorizar uno o más de una cantidad de paquetes de autenticación que llega al dispositivo 120 de control de acceso, una cantidad de paquetes de autenticación perdidos, y una tasa de pérdida de paquetes de los paquetes de autenticación. Se considera que una condición para restringir la tasa a la que se recibe el paquete de inicio de autenticación se satisface sólo cuando se encuentra, monitorizando, que por unidad de tiempo, la cantidad de paquetes de autenticación que llegan al dispositivo 120 de control de acceso es excesivamente grande, la cantidad de paquetes de autenticación perdidos es excesivamente grande, o la tasa de pérdida de paquetes de los paquetes de autenticación es excesivamente grande, y después, se restringe la tasa a la que el dispositivo 120 de control de acceso recibe el paquete de inicio de autenticación

En otro aspecto, cuando se produce un efecto avalancha en el proceso de autenticación, disminuye una cantidad de terminales que realizan el acceso de manera exitosa en la unidad de tiempo. La cantidad de terminales que realizan el acceso de manera exitosa en la unidad de tiempo usando el dispositivo 120 de control de acceso se puede monitorizar también. Se restringe La tasa a la que el dispositivo 120 de control de acceso recibe el paquete de inicio de autenticación sólo cuando se encuentra, monitorizando, que la cantidad de terminales que realizan el acceso de manera exitosa en la unidad de tiempo usando el dispositivo 120 de control de acceso es menor que un umbral.

Para mejorar la exactitud de la detección y reducir la probabilidad de detección errónea, las condiciones en los dos aspectos anteriores se pueden combinar, y la tasa del paquete de inicio de autenticación se restringe sólo cuando los dos tipos (paquetes de autenticación de monitorización y terminales de monitorización que realizan el acceso de manera exitosa) de condiciones se satisfacen.

En referencia a la FIG. 2, que muestra un diagrama de flujo de método de un método de control de la autenticación según una realización de la presente invención. El método de control de la autenticación se puede aplicar al dispositivo 120 de control de acceso en el entorno de implementación mostrado en la FIG. 1. El método de control de la autenticación puede incluir:

Etapa 201: Detectar si un paquete que llega a un dispositivo de control de acceso es un paquete de inicio de autenticación, donde el paquete de inicio de autenticación se usa para iniciar un proceso de autenticación de un terminal que envía el paquete de inicio de autenticación.

Etapa 202: Restringir una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación. Al recibir un paquete, el dispositivo de control de acceso almacena primero de manera temporal el paquete recibido, y analiza una cabecera de paquete del paquete; si determina, analizando la cabecera de paquete, recibir el paquete, el dispositivo de control de acceso envía el paquete a una unidad de procesamiento (por ejemplo, una unidad de procesamiento central) del dispositivo de control de acceso para realizar el procesamiento posterior. Por lo tanto, en las realizaciones de la presente invención, un paquete que llega a un dispositivo de control de acceso se refiere a un paquete almacenado de manera temporal por el dispositivo de control de acceso, y la recepción de un paquete se refiere al envío de un paquete cuando se determina que el procesamiento posterior necesita ser realizado sobre el paquete, por ejemplo, reenviando el paquete o enviando el paquete a una unidad de procesamiento.

En conclusión, según el método de control de autenticación proporcionado en esta realización de la presente invención, se detecta si un paquete que llega a un dispositivo de control de acceso es un paquete de inicio de autenticación, y se restringe una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación. La tasa a la que se recibe el paquete de inicio de autenticación se restringe para controlar una cantidad de terminales que entran en una autenticación posterior, lo que evita un efecto avalancha de autenticación inalámbrica provocado cuando una cantidad excesivamente grande de terminales entran de manera simultánea a una autenticación posterior, y asegura que un terminal que actualmente ya realiza una autenticación de acceso posterior puede completar un proceso de autenticación completo sin problemas, consiguiendo de este modo un efecto de mejora de la eficiencia de autenticación del sistema.

Para una descripción adicional del método de control de autenticación mostrado en la FIG. 2, se hace referencia a la FIG. 3A, que muestra un diagrama de flujo de método de un método de control de la autenticación según otra realización de la presente invención. El método de control de la autenticación se puede aplicar al dispositivo 120 de control de acceso en el entorno de implementación mostrado en la FIG. 1. El método de control de autenticación puede incluir:

Etapa 301: Restringir una tasa a la que un dispositivo de control de acceso recibe un paquete de autenticación, donde el paquete de autenticación es un paquete usado para la autenticación de acceso de un terminal.

En esta realización de la presente invención, el dispositivo de control de acceso realiza primero una restricción de tasa general sobre todos los paquetes de autenticación a ser recibidos, esto es, restringe una tasa a la que los paquetes de autenticación se envían a una unidad de procesamiento (por ejemplo, una unidad de procesamiento central) del dispositivo de control de acceso, para evitar el impacto sobre un plano e control del dispositivo de control de acceso provocado por una cantidad excesivamente grande de paquetes de autenticación.

El dispositivo de control de acceso puede realizar la restricción de tasa general sobre los paquetes de autenticación a ser recibidos usando un mecanismo de cubo de identificadores. Un algoritmo de cubo de identificadores es un algoritmo que se usa a menudo en el conformado del tráfico de red y en la restricción de tasa. Normalmente, el algoritmo de cubo de identificadores se usa para controlar la cantidad de datos recibidos y permitir el envío de datos masivos.

Etapa 302: Monitorizar un estado de recepción de paquetes.

En esta realización de la presente invención, el estado de recepción de paquetes puede incluir al menos uno de una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo, una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo, o una relación de una cantidad de paquetes de autenticación que son descartados por el dispositivo de control

de acceso en por unidad de tiempo con una cantidad de paquetes de autenticación que llegan el dispositivo de control de acceso por unidad de tiempo.

Etapa 303: Detectar si el estado de recepción de paquetes satisface una primera condición predeterminada.

En esta realización de la presente invención, la primera condición predeterminada incluye una de las siguientes condiciones:

la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es mayor que un primer umbral

la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso al dispositivo de control de acceso por unidad de tiempo es mayor que un segundo umbral; o

la relación de la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo con la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es mayor que un tercer umbral.

En esta realización de la presente invención, para aliviar la carga de cálculo en el dispositivo de control de acceso y reducir los recursos de procesamiento, se puede detectar el estado de recepción de paquetes satisface la primera condición predeterminada, y cuando el estado de recepción de paquetes satisface la primera condición predeterminada, se puede considerar que se satisface una condición para restringir el paquete de inicio de autenticación. El paquete de inicio de autenticación se usa para iniciar un proceso de autenticación de un terminal que envía el paquete de inicio de autenticación.

El primer umbral involucrado en la primera condición predeterminada se puede establecer según una capacidad de cálculo del dispositivo de control de acceso, por ejemplo, el primer umbral se puede establecer a la mayor cantidad de paquetes de autenticación que pueden ser procesados por el dispositivo de control de acceso por unidad de tiempo. Tanto el segundo umbral como el tercer umbral que se involucran en la primera condición predeterminada se pueden establecer a 0, o se pueden establecer respectivamente a valores mayores que 0.

Etapa 304: Monitorizar una cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso.

Etapa 305: Detectar si la cantidad de terminales que se autentican de manera satisfactoria por unidad de tiempo usando el dispositivo de control de acceso es mayor que un cuarto umbral.

La unidad de tiempo en la etapa 304 y la etapa 305 puede ser la misma que o diferente de la unidad de tiempo en la etapa 302 y la etapa 303.

En una aplicación real, ya que existen los datos de masivos, puede aparecer un caso en el que una gran cantidad de paquetes de autenticación llegan al dispositivo de control de acceso o se descartan una gran cantidad de paquetes de autenticación por el dispositivo de control de acceso cuando no se produce efecto avalancha o autenticación inalámbrica. Por lo tanto, es inexacto determinar, según sólo una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso o a una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso, si se produce un efecto avalancha. Por lo tanto, en la solución mostrada en esta realización de la presente invención, para mejorar la exactitud de la determinación, se puede determinar además, con referencia a la cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso, si se produce un efecto avalancha, esto es, se considera que se satisface una condición para restringir la tasa a la que se recibe el paquete de inicio de autenticación sólo cuando la cantidad de terminales que se autentica de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso es mayor que el cuarto umbral.

Etapa 306: Cuando el estado de recepción de paquetes satisface la primera condición predeterminada, y la cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso es mayor que el cuarto umbral, detectar si un paquete de autenticación que llega al dispositivo de control de acceso satisface una segunda condición predeterminada, y si el paquete de autenticación que llega al dispositivo de control de acceso satisface la segunda condición predeterminada, determina que el paquete de autenticación que llega al dispositivo de control de acceso es un paquete de inicio de autenticación.

La segunda condición predeterminada es una de las siguientes condiciones:

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación Extensible EAP, un campo de tipo de paquete en el paquete EAP es 1;

cuando el paquete de autenticación es un paquete EAP, en el paquete EAP, un campo de tipo de paquete es 0, un campo de tipo de cuerpo de paquete es 2, y un campo de tipo de autenticación es 1;

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Desafío-Respuesta, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de

tipo es 1, y un campo chap es 0; o

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Clave PAP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 3, y un campo pap es 1.

Para autenticación EAP, se hace referencia de la FIG. 3B a la FIG. 3E. La FIG. 3B muestra un diagrama de flujo de interacciones de autenticación EAP. En la FIG. 3B, un paquete de inicio de autenticación es un paquete de INICIO-EAP o un paquete IDENTIDAD- EAP entre los paquetes EAP. En referencia a la FIG. 3C, que muestra un diagrama de una estructura de encapsulación de una paquete EAP. Un campo tipo en el diagrama de la estructura de encapsulación del paquete EAP es un campo de tipo de paquete en el paquete EAP. Un valor del campo de tipo de paquete se usa para indicar un tipo de trama de datos incluidos en un Cuerpo de Paquete. Los valores del campo de tipo de paquete en el paquete EAP y los tipos de tramas de datos indicados por los valores se muestran en la Tabla 1.

Tabla 1

Valor	Tipo de trama de datos
0 (0x00)	Paquete EAP: trama de información de autenticación
1 (0x01)	Inicio-EAPOL: trama de inicio de autenticación
2 (0x02)	Desconexión-EAPOL: trama de solicitud de desconexión

Un paquete de INICIO-EAP incluye una trama de inicio de autenticación. Por lo tanto, cuando un paquete de autenticación es un paquete EAP, y un campo de tipo de paquete en el paquete EAP es 1 (o representado como 0x01), el paquete es un paquete INICIO-EAP.

En referencia a la FIG. 3D, que muestra un diagrama de formato de un cuerpo de paquete (Cuerpo de Paquete) de un paquete EAP si un campo de tipo de paquete en el paquete EAP es 0. Un campo Código en el cuerpo de paquete es un campo tipo de cuerpo. Los valores del campo tipo de cuerpo de paquete y tipos de cuerpos de paquete indicados por los valores se muestran en la Tabla 2.

Tabla 2

Valor	Tipo de cuerpo de paquete
1	Solicitud: solicitud
2	Respuesta: respuesta
3	Éxito: éxito
4	Fallo: fallo

Cuando un tipo de cuerpo de paquete es Solicitud o Respuesta, un diagrama de formato de un formato de un cuerpo datos (Datos) en el cuerpo de paquete se puede mostrar en la FIG. 3E. Un campo tipo en el campo datos es un campo tipo de autenticación. Los valores del campo tipo de autenticación y de los tipos de autenticación indicados por los valores se muestran en la Tabla 3.

Tabla 3

Valor	Tipo de autenticación
1	Identificador: consulta de la identidad de un extremo
2	Notificación: alarma o aviso
…	…

Un paquete de IDENTIDAD-EAP (identidad) incluye una trama de información de autenticación, y un tipo de cuerpo de paquete del paquete IDENTIDAD-EAP (identidad) es Respuesta; y un tipo de autenticación del paquete de IDENTIDAD-EAP (identidad) es Identificador. Por lo tanto, cuando un paquete de autenticación es un paquete EAP, un campo de tipo de paquete en el paquete EAP es 0 (o representado como 0x00), un campo tipo de cuerpo de paquete es 2, y un campo tipo de autenticación es 1, el paquete es un paquete IDENTIDAD-EAP (identidad).

Para la autenticación de portal cautivo, en referencia a la FIG. 3F, que muestra un diagrama de flujo de la interacción de la autenticación de portal cautivo. Un paquete que transporta la autenticación de portal cautivo es un paquete del Protocolo de Datagramas de Usuario (en inglés: User Datagram Protocol, UDP). Se puede determinar, según un número de puerto de un paquete UDP, que una carga útil en el paquete UDP es un paquete del Protocolo de Autenticación por Desafío-Respuesta (en inglés: Challenge Handshake Authentication Protocol, CHAP para abreviar) o un paquete del Protocolo de Autenticación por Clave (en inglés: Password Authentication Protocol, PAP para abreviar). En la FIG. 3F, un paquete de inicio de autenticación es un paquete CHAP (esto es, un paquete de solicitud de DESAFÍO) o un paquete de solicitud de autenticación PAP. Cuando el paquete CHAP es un paquete de solicitud de DESAFÍO, en el paquete CHAP, un campo ver es 2, un campo tipo es 1, y un campo CHAP es 0. Cuando un paquete PAP es un paquete de solicitud de autenticación PAP, en el paquete PAP, un campo ver es 2, un campo de tipo es 3, y un campo pap es 1.

Etapa 307: Restringir una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación. Específicamente, cuando se restringe la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, se puede restringir una cantidad de paquetes de inicio de autenticación que son enviados por el dispositivo de control de acceso a una unidad de procesamiento por unidad de tiempo, o se puede restringir una cantidad de datos de paquetes de inicio de autenticación que son enviados por el dispositivo de control de acceso a una unidad de procesamiento por unidad de tiempo. El proceso de restricción puede ser implementado también usando un mecanismo de cubo de identificadores, que no se describe de manera repetida en la presente memoria.

Etapa 308: Continuar para monitorizar el estado de recepción de paquetes, y detectar si el estado de recepción de paquetes satisface una tercera condición predeterminada.

La tercera condición predeterminada que se satisface incluye uno de lo siguiente:

la cantidad de paquetes de autenticación que llega al dispositivo de control de acceso por unidad de tiempo es menor que un quinto umbral, donde el quinto umbral es menor que el primer umbral;

la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo es menor que un sexto umbral, donde el sexto umbral es menor que el segundo umbral; o

la relación de la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo a la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es menor que un séptimo umbral, donde el séptimo umbral es menor que el tercer umbral.

Etapa 309: Cancelar la restricción sobre la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación.

Después de que se restrinja la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, el estado de recepción de paquetes del dispositivo de control de acceso puede continuar para ser monitorizada. Cuando se encuentra, mediante la monitorización, que la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo disminuye por debajo de un umbral, o que la cantidad de paquetes de autenticación que se descartan por unidad de tiempo disminuye por debajo de un umbral, o que la relación de la cantidad de paquetes de autenticación que se descartan por unidad de tiempo con la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo disminuye por debajo de un umbral, se puede determinar que una cantidad de terminales que actualmente realizan la autenticación de acceso es ya relativamente pequeña. En este caso, se puede cancelar la restricción sobre la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, para aliviar la carga de cálculo en el dispositivo de control de acceso y reducir los recursos de procesamiento.

En conclusión, según el método de control de autenticación proporcionado en esta realización de la presente invención, se detecta si un paquete que llega a un dispositivo de control de acceso es un paquete de inicio de autenticación, y se restringe una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación. La tasa a la que el paquete de inicio de autenticación se recibe se restringe para controlar una cantidad de terminales que entran en la autenticación posterior, lo que evita un efecto avalancha de autenticación inalámbrica provocado cuando una gran cantidad de terminales entran de manera simultánea en la autenticación posterior, y asegura que un terminal que actualmente ya realiza la autenticación de acceso posterior puede completar un proceso de autenticación completa sin problemas, consiguiente de este modo un efecto de mejora de la eficiencia de la autenticación del sistema

Además, según el método de control de autenticación proporcionado en esta realización de la presente invención, se

monitoriza un estado de recepción de paquetes, y cuando se detecta que el estado de recepción de paquetes satisface una primera condición predeterminada, se restringe la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, consiguiendo de este modo los efectos de aliviar la carga de cálculo en el dispositivo de control de acceso y reducir los recursos de procesamiento.

Además, según el método de control de autenticación proporcionado en esta realización de la presente invención, se restringe la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación sólo cuando se detecta que una cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso es mayor que un cuarto umbral, consiguiendo de este modo los efectos de mejora de la exactitud de detección y reducción de una probabilidad de detección errónea.

En referencia a la FIG. 4, que muestra un diagrama estructural de un dispositivo de control de acceso según una realización de la presente invención. El dispositivo de control de acceso se puede implementar como el dispositivo 120 de control de acceso en el entorno de implementación mostrado en la FIG. 1. El dispositivo de control de acceso puede incluir:

un módulo 401 de detección, configurado para detectar si un paquete que llega al dispositivo de control de acceso es un paquete de inicio de autenticación, donde el paquete de inicio de autenticación se usa para iniciar un proceso de autenticación de un terminal que envía el paquete de inicio de autenticación; y

un módulo 402 de restricción, configurado para restringir una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación.

En conclusión, según el dispositivo de control de acceso proporcionado en esta realización de la presente invención, se detecta si un paquete que llega al dispositivo de control de acceso es un paquete de inicio de autenticación, y se restringe una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación. Se restringe la tasa a la que el paquete de inicio de autenticación es recibido para controlar una cantidad de terminales que entran en la autenticación posterior, lo que evita un efecto avalancha de la autenticación inalámbrica provocado cuando una cantidad excesivamente grande de terminales entran en la autenticación posterior de manera simultánea, y asegura que un terminal que actualmente ya realiza la autenticación de acceso posterior pueda completar un proceso de autenticación sin problemas, consiguiendo de este modo un efecto de mejora de la eficiencia de la autenticación del sistema

Para una descripción adicional del dispositivo de control de autenticación mostrado en la FIG. 4, en referencia a la FIG. 5, que muestra un diagrama estructural de un dispositivo de control de acceso según otra realización de la presente invención. El dispositivo de control de acceso se puede implementar como el dispositivo 120 de control de acceso en el entorno de implementación mostrado en la FIG. 1. El dispositivo de control de acceso puede incluir:

un módulo 401 de detección, configurado para detectar si un paquete que llega al dispositivo de control de acceso es un paquete de inicio de autenticación, donde el paquete de inicio de autenticación se usa para iniciar un proceso de autenticación de un terminal que envía el paquete de inicio de autenticación; y

un módulo 402 de restricción, configurado para restringir una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación.

De manera opcional, el módulo 402 de restricción se configura para restringir la tasa a al que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, sólo cuando un estado de recepción de paquetes satisface una primera condición predeterminada, donde la primera condición predeterminada incluye una de las siguientes condiciones:

una cantidad de paquetes de autenticación que llega al dispositivo de control de acceso por unidad de tiempo es mayor que un primer umbral;

una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo es mayor que un segundo umbral; o

una relación de una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo con una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es mayor que un tercer umbral.

De manera opcional, el módulo 402 de restricción se configura para restringir la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, sólo cuando una cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso es mayor que un cuarto umbral.

De manera opcional, el módulo 401 de detección se configura específicamente para detectar si un paquete de autenticación que llega al dispositivo de control de acceso satisface una segunda condición predeterminada, y si el paquete de autenticación que llega al dispositivo de control de acceso satisface la segunda condición predeterminada, determinar que el paquete de autenticación que llega al dispositivo de control de acceso es un paquete de inicio de

autenticación, donde la segunda condición predeterminada es una de las siguientes condiciones:

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación Extensible EAP, un campo de tipo de paquete en el paquete EAP es 1;

cuando el paquete de autenticación es un paquete EAP, en el paquete EAP, un campo de tipo de paquete es 0, un campo de tipo de cuerpo de paquete es 2, y un campo de tipo de autenticación es 1;

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Desafío-Respuesta, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 1, y un campo chap es 0; o

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Clave PAP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 3, y un campo pap es 1.

Opcionalmente, el dispositivo de control de acceso incluye, además:

un módulo 403 de cancelación, configurado para: cuando una tercera condición predeterminada se satisface, cancelar la restricción realizada por el módulo de restricción sobre la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, donde la tercera condición predeterminada que se satisface incluye uno de lo siguiente:

la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es menor que un quinto umbral, donde el quinto umbral es menor que el primer umbral;

la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo es menor que un sexto umbral, donde el sexto umbral es menor que el segundo umbral; o

la relación de la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo con la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es menor que un séptimo umbral, donde el séptimo umbral es menor que el tercer umbral.

En conclusión, según el dispositivo de control de acceso proporcionado en esta realización de la presente invención, se detecta si un paquete que llega al dispositivo de control de acceso es un paquete de inicio de autenticación, y se restringe una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación. Se restringe la tasa a la que el paquete de inicio de autenticación es recibido para controlar una cantidad de terminales que entran en la autenticación posterior, lo que evita un efecto avalancha de la autenticación inalámbrica provocado cuando una cantidad excesivamente grande de terminales entran de manera simultánea a la autenticación posterior, y asegura que un terminal que actualmente ya realiza la autenticación de acceso posterior puede completar un proceso de autenticación completo sin problemas, consiguiendo de este modo un efecto de mejora de la eficiencia de la autenticación del sistema.

Además, según el dispositivo de control de acceso proporcionado en esta realización de la presente invención, se monitoriza un estado de recepción de paquetes, y cuando se detecta que el estado de recepción de paquetes satisface una primera condición predeterminada, se restringe la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, consiguiendo de este modo los efectos de aliviar la carga de cálculo en el dispositivo de control de acceso y reducir los recursos de procesamiento.

Además, según el dispositivo de control de acceso proporcionado en esta realización de la presente invención, se restringe la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación sólo cuando se detecta que una cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso es mayor que un cuarto umbral, consiguiendo de este modo los efectos de mejora de la exactitud de detección y reducción de la probabilidad de detección errónea.

En referencia a la FIG. 6, que muestra un diagrama de bloques de un dispositivo de red según una realización de la presente invención. Un dispositivo 600 de red puede ser el anterior dispositivo 120 de control de acceso en el entorno de red mostrado en la FIG. 1. El dispositivo de red puede incluir: un adaptador 601 de red, una unidad 602 de procesamiento central, y una memoria 603. El adaptador 601 de red incluye un procesador 601a de paquetes (en inglés: packet processor) y una interfaz 601b de red. Después de analizar un paquete de autenticación que llega al dispositivo de red, el procesador 601a de paquetes envía el paquete de autenticación a la unidad 602 de procesamiento central. La unidad 602 de procesamiento central ejecuta una instrucción almacenada en la memoria 603, para procesar el paquete de autenticación. La interfaz 601b de red puede incluir una interfaz de red por cable, por ejemplo, una interfaz Ethernet, o puede incluir una interfaz de red inalámbrica.

El procesador 601a de paquetes se configura para detectar si un paquete que llega al dispositivo de red es un paquete de inicio de autenticación, donde el paquete de inicio de autenticación se usa para iniciar un proceso de autenticación

de un terminal que envía el paquete de inicio de autenticación; y

el procesador 601a de paquetes se configura para restringir una tasa a la que el dispositivo de red recibe el paquete de inicio de autenticación.

De manera opcional, el procesador 601a de paquetes se configura para restringir la tasa a la que el dispositivo de red recibe el paquete de inicio de autenticación, sólo cuando la unidad 602 de procesamiento central detecta que un estado de recepción de paquetes satisface una primera condición predeterminada, donde la primera condición predeterminada incluye una de las siguientes condiciones:

una cantidad de paquetes de autenticación que llegan al dispositivo de red por unidad de tiempo es mayor que un primer umbral;

una cantidad de paquetes de autenticación que son descartados por el dispositivo de red por unidad de tiempo es mayor que un segundo umbral; o

una relación de una cantidad de paquetes de autenticación que son descartados por el dispositivo de red por unidad de tiempo con una cantidad de paquetes de autenticación que llegan al dispositivo de red por unidad de tiempo es mayor que un tercer umbral.

De manera opcional, el procesador 601a de paquetes se configura para restringir la tasa a la que el dispositivo de red recibe el paquete de inicio de autenticación, sólo cuando la unidad 602 de procesamiento central detecta que una cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de red es mayor que un cuarto umbral.

De manera opcional, el procesador 601a de paquetes se configura de manera específica para detectar si un paquete de autenticación que llega al dispositivo de red satisface una segunda condición predeterminada, y si el paquete de autenticación que llega al dispositivo de red satisface la segunda condición predeterminada, determinar que el paquete de autenticación que llega al dispositivo de red es un paquete de inicio de autenticación, donde la segunda condición predeterminada es una de las siguientes condiciones:

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación Extensible EAP, un campo de tipo de paquete en el paquete EAP es 1;

cuando el paquete de autenticación es un paquete EAP, en el paquete EAP, un campo de tipo de paquete es 0, un campo de tipo de cuerpo de paquete es 2, y un campo de tipo de autenticación es 1;

cuando el paquete de autenticación es un paquete del Protocolo de Datagramas de Usuario UDP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 1, y un campo chap es 0; o

cuando el paquete de autenticación es un paquete UDP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 3, y un campo pap es 1.

De manera opcional, el procesador 601a de paquetes se configura para: cuando la unidad 602 de procesamiento central detecta que una tercera condición predeterminada se satisface, cancelar la restricción sobre la tasa a la que el dispositivo de red recibe el paquete de inicio de autenticación, donde la tercera condición predeterminada que se satisface incluye uno de lo siguiente:

la cantidad de paquetes de autenticación que llegan al dispositivo de red por unidad de tiempo es menor que un quinto umbral, donde el quinto umbral es menor que el primer umbral;

la cantidad de paquetes de autenticación que son descartados por el dispositivo de red por unidad de tiempo es menor que un sexto umbral, donde el sexto umbral es menor que el segundo umbral; o

la relación de una cantidad de paquetes de autenticación que son descartados por el dispositivo de red por unidad de tiempo con la cantidad de paquetes de autenticación que llegan al dispositivo de red por unidad de tiempo es menor que un séptimo umbral, donde el séptimo umbral es menor que el tercer umbral.

En conclusión, cuando el dispositivo de red proporcionado en esta realización de la presente invención se implementa como un dispositivo de control de acceso, se detecta si un paquete que llega al dispositivo de red es un paquete de inicio de autenticación, y se restringe una tasa a la que el dispositivo de red recibe el paquete de inicio de autenticación. Se restringe la tasa a la que se recibe el paquete de inicio de autenticación para controlar una cantidad de terminales que entran en la autenticación posterior, lo que evita un efecto avalancha de la autenticación inalámbrica provocado cuando una cantidad excesivamente grande de terminales entran de manera simultánea en la autenticación posterior, y asegura que un terminal que actualmente ya realiza la autenticación de acceso posteriores puede completar un proceso de autenticación completo sin problemas, consiguiendo de este modo un efecto de mejora de la eficiencia de la autenticación del sistema.

Además, cuando el dispositivo de red proporcionado en esta realización de la presente invención es implementado como un dispositivo de control de acceso, se monitoriza un estado de recepción de paquetes, y cuando se detecta que el estado de recepción de paquetes satisface una primera condición predeterminada, se restringe la tasa a la que el dispositivo de red recibe el paquete de inicio de autenticación, consiguiendo de este modo los efectos de aliviar la carga de cálculo en el dispositivo de control de acceso y reducir los recursos de procesamiento.

Además, cuando el dispositivo de red proporcionado en esta realización de la presente invención se implementa como un dispositivo de control de acceso, se restringe la tasa a la que el dispositivo de red recibe el paquete de inicio de autenticación sólo cuando se detecta que una cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de red es mayor que un cuarto umbral, consiguiendo de este modo los efectos de mejora de la exactitud de detección y reducción de una probabilidad de detección errónea.

Se debería observar que cuando el dispositivo de control de acceso proporcionado en las realizaciones anteriores controla un paquete de autenticación, la división de los módulos funcionales anteriores se usa simplemente como un ejemplo para la ilustración. En la solicitud real, las funciones anteriores se pueden asignar a e implementar por diferentes módulos funcionales según un requisito, esto es, una estructura interna del dispositivo se divide en diferentes módulos funcionales para implementar todas o algunas de las funciones descritas anteriormente. Además, las realizaciones del dispositivo de control de acceso y del método de control de la autenticación que se proporcionan en las realizaciones anteriores pertenecen a un mismo concepto inventivo, y para los detalles sobre un proceso de implementación específico, se hace referencia a las realizaciones del método, que no se describen de manera repetida en la presente memoria.

Los números de secuencia de las realizaciones anteriores de la presente invención son simplemente para propósitos ilustrativos, y no están destinadas para indicar prioridades de las realizaciones.

Una persona de experiencia ordinaria en la técnica puede entender que todas o algunas de las etapas de las realizaciones pueden ser implementados por hardware o un programa que da instrucciones relacionado con un hardware. El programa se puede almacenar en un medio de almacenamiento legible por ordenador. El medio de almacenamiento puede incluir: una memoria de sólo lectura, un disco magnético, un disco óptico o similar.

Las descripciones anteriores son simplemente maneras de implementación ejemplares de la presente invención, pero no están destinadas a limitar el alcance de protección de la presente invención. Cualquier variación o reemplazo fácilmente ideados por una persona experta en la técnica dentro del alcance técnico descrito en la presente invención caerá dentro del alcance de protección de la presente invención. Por lo tanto, el alcance de protección de la presente invención estará sujeto al alcance de protección de las reivindicaciones.

REIVINDICACIONES

1. Un dispositivo de control de acceso, en donde el dispositivo de control de acceso comprende:

un módulo (402) de restricción, configurado para restringir una tasa a la que el dispositivo de control de acceso recibe un paquete de autenticación;

un módulo (401) de detección, configurado para detectar si un paquete que llega al dispositivo de control de acceso es un paquete de inicio de autenticación, en donde el paquete de inicio de autenticación se usa para iniciar un proceso de autenticación de un terminal que envía el paquete de inicio de autenticación y en donde el paquete de autenticación es un paquete usado para la autenticación de acceso del terminal; y en donde

el módulo (402) de restricción se configura además para restringir una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación.

2. El dispositivo de control de acceso según la reivindicación 1, en donde

el módulo de restricción se configura para restringir la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, sólo cuando un estado de recepción de paquetes satisface una primera condición predeterminada, en donde

la primera condición predeterminada comprende una de las siguientes condiciones:

una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es mayor que un primer umbral;

una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo es mayor que un segundo umbral; o

una relación de una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo con una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es mayor que un tercer umbral.

3. El dispositivo de control de acceso según la reivindicación 1 o 2, en donde el módulo de restricción se configura para restringir la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, sólo cuando una cantidad de terminales que se autentican con éxito por unidad de tiempo usando el dispositivo de control de acceso es mayor que un cuarto umbral.

4. El dispositivo de control de acceso según una cualquiera de las reivindicaciones 1 a 3, en donde el módulo de detección se configura específicamente para detectar si un paquete de autenticación que llega al dispositivo de control de acceso satisface una segunda condición predeterminada, y si el paquete de autenticación que llega al dispositivo de control de acceso satisface la segunda condición predeterminada, determinar que un paquete de autenticación que llega al dispositivo de control de acceso es un paquete de inicio de autenticación, en donde

la segunda condición predeterminada es una de las siguientes condiciones:

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación Extensible, EAP, un campo de tipo de paquete en el paquete EAP es 1;

cuando el paquete de autenticación es un paquete EAP, en el paquete EAP, un campo de tipo de paquete es 0, un campo de tipo de cuerpo de paquete es 2, y un campo de tipo de autenticación es 1;

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Desafío-Respuesta, CHAP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 1, y un campo chap es 0;o

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Clave, PAP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 3, y un campo pap es 1.

5. El dispositivo de control de acceso según una cualquiera de las reivindicaciones 1 a 4, en donde el dispositivo de control de acceso comprende, además:

un módulo de cancelación, configurado para: cuando una tercera condición predeterminada se satisface, cancelar la restricción realizada por el módulo de restricción sobre la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, en donde

la tercera condición predeterminada que se satisface comprende uno de lo siguiente:

la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es menor

que un quinto umbral, en donde el quinto umbral es menor que el primer umbral;

la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo es menor que un sexto umbral, en donde el sexto umbral es menor que el segundo umbral; o

la relación de la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo con la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es menor que el séptimo umbral, en donde el séptimo umbral es menor que el tercer umbral.

6. Un método de control de autenticación, en donde el método comprende:

restringir (301) una tasa a la que el dispositivo de control de acceso recibe un paquete de autenticación;

detectar (306) si un paquete que llega a un dispositivo de control de acceso es un paquete de inicio de autenticación, en donde el paquete de inicio de autenticación se usa para iniciar un proceso de autenticación de un terminal que envía el paquete de inicio de autenticación y en donde el paquete de autenticación es un paquete usado para la autenticación de acceso del terminal; y

restringir (307) una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación.

7. El método según la reivindicación 6, en donde la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación está restringido sólo cuando un estado de recepción de paquetes satisface una primera condición predeterminada, en donde

la primera condición predeterminada comprende una de las siguientes condiciones:

una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es mayor que un primer umbral;

una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo es mayor que un segundo umbral; o

una relación de una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo con una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es mayor que un tercer umbral.

8. El método según la reivindicación 6 o 7, en donde restringir una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación comprende:

restringir la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación, sólo cuando una cantidad de terminales que se autentican con éxito por unidad de tiempo usando el dispositivo de control de acceso es mayor que un cuarto umbral.

9. El de autenticación comprende:

detectar si un paquete de autenticación que llega al dispositivo de control de acceso satisface una segunda condición predeterminada, y si el paquete de método según una cualquiera de las reivindicaciones 6 a 8, en donde la detección de si un paquete que llega a un dispositivo de control de acceso es un paquete de inicio autenticación que llega a dispositivo de control de acceso satisface la segunda condición predeterminada, determinar que el paquete de autenticación que llega al dispositivo de control de acceso es un paquete de inicio de autenticación, en donde

la segunda condición predeterminada es una de las siguientes condiciones:

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación Extensible, EAP, un campo de tipo de paquete en el paquete EAP es 1;

cuando el paquete de autenticación es un paquete EAP, en el paquete EAP, un campo de tipo de paquete es 0, un campo de tipo de cuerpo de paquete es 2, y un campo de tipo de autenticación es 1;

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Desafío-Respuesta, CHAP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 1, y un campo chap es 0;o

cuando el paquete de autenticación es un paquete del Protocolo de Autenticación por Clave, PAP, en el paquete de autenticación que llega al dispositivo de control de acceso, un campo ver es 2, un campo de tipo es 3, y un campo pap es 1.

10. El método según una cualquiera de las reivindicaciones 6 a 9, en donde el método comprende, además:

cuando se satisface una tercera condición predeterminada, cancelar (309) la restricción sobre la tasa a la que el

dispositivo de control de acceso recibe el paquete de inicio de autenticación, en donde

la tercera condición predeterminada que se satisface comprende uno de lo siguiente:

la cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es menor que un quinto umbral, en donde el quinto umbral es menor que el primer umbral;

la cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo es menor que un sexto umbral, en donde el sexto umbral es menor que el segundo umbral; o

la relación de una cantidad de paquetes de autenticación que son descartados por el dispositivo de control de acceso por unidad de tiempo con una cantidad de paquetes de autenticación que llegan al dispositivo de control de acceso por unidad de tiempo es menor que un séptimo umbral, en donde el séptimo umbral es menor que el tercer umbral.

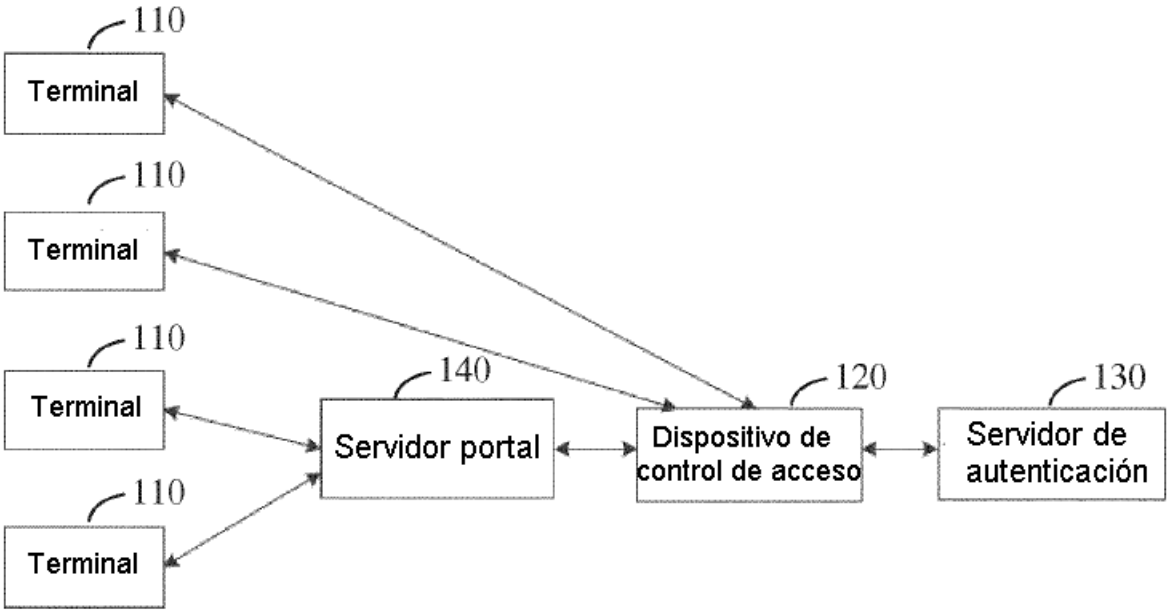
110
Terminal
110
Terminal
110
Terminal
110
Terminal
140
Servidor portal
120
Dispositivo de control de acceso
130
Servidor de autenticación

FIG. 1

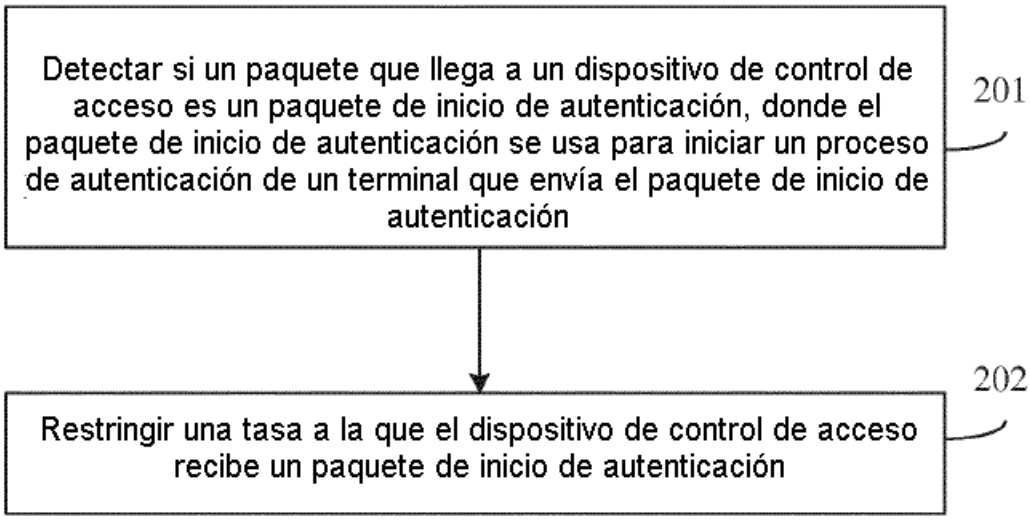
Detectar si un paquete que llega a un dispositivo de control de acceso es un paquete de inicio de autenticación, donde el paquete de inicio de autenticación se usa para iniciar un proceso de autenticación de un terminal que envía el paquete de inicio de autenticación
201
Restringir una tasa a la que el dispositivo de control de acceso recibe un paquete de inicio de autenticación
202

FIG. 2

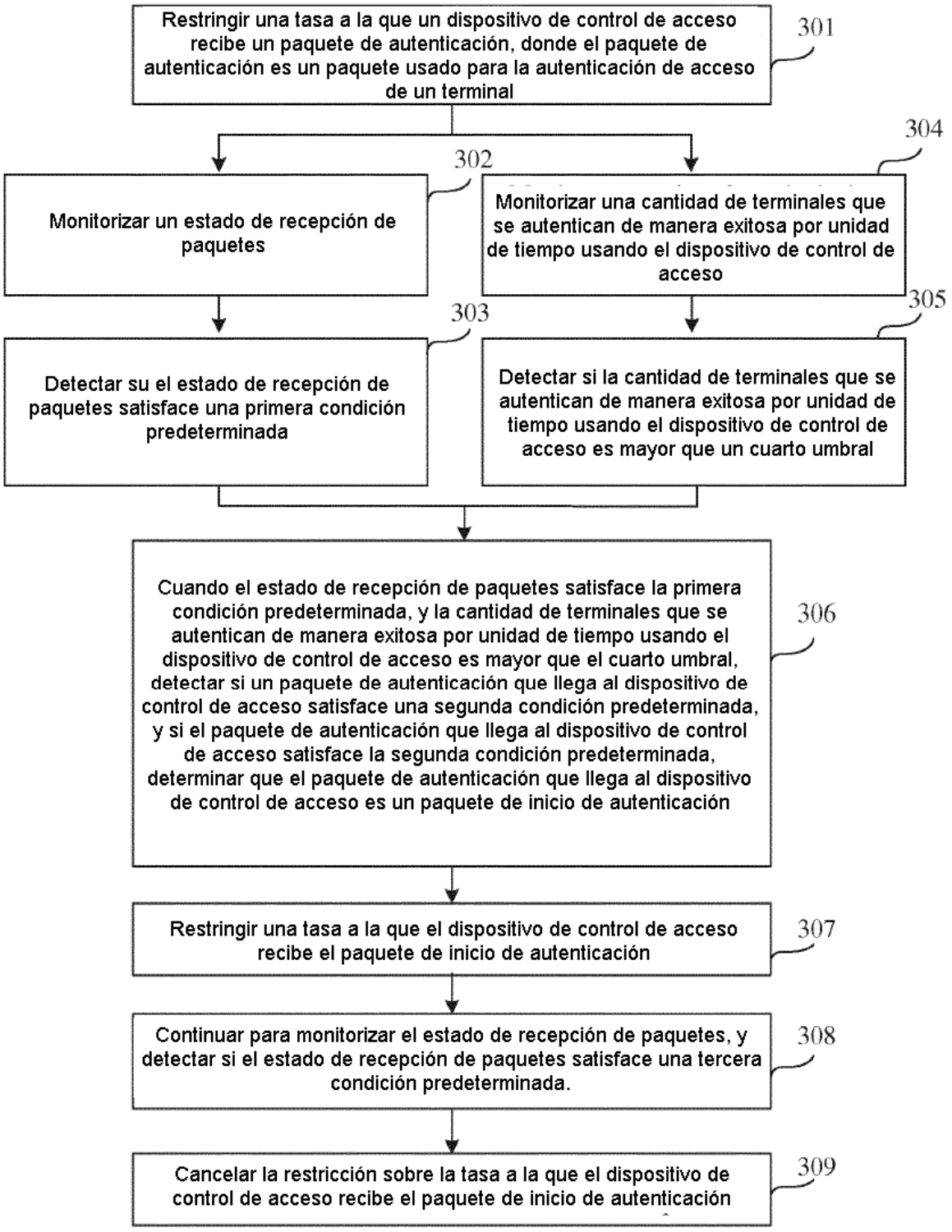
Restringir una tasa a la que un dispositivo de control de acceso recibe un paquete de autenticación, donde el paquete de autenticación es un paquete usado para la autenticación de acceso de un terminal
301
304
302
Monitorizar un estado de recepción de paquetes
Monitorizar una cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso
305
303
Detectar su el estado de recepción de paquetes satisface una primera condición predeterminada
Detectar si la cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso es mayor que un cuarto umbral
Cuando el estado de recepción de paquetes satisface la primera condición predeterminada, y la cantidad de terminales que se autentican de manera exitosa por unidad de tiempo usando el dispositivo de control de acceso es mayor que el cuarto umbral, detectar si un paquete de autenticación que llega al dispositivo de control de acceso satisface una segunda condición predeterminada, y si el paquete de autenticación que llega al dispositivo de control de acceso satisface la segunda condición predeterminada, determinar que el paquete de autenticación que llega al dispositivo de control de acceso es un paquete de inicio de autenticación
306
Restringir una tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación
307
Continuar para monitorizar el estado de recepción de paquetes, y detectar si el estado de recepción de paquetes satisface una tercera condición predeterminada.
308
Cancelar la restricción sobre la tasa a la que el dispositivo de control de acceso recibe el paquete de inicio de autenticación
309

FIG. 3A

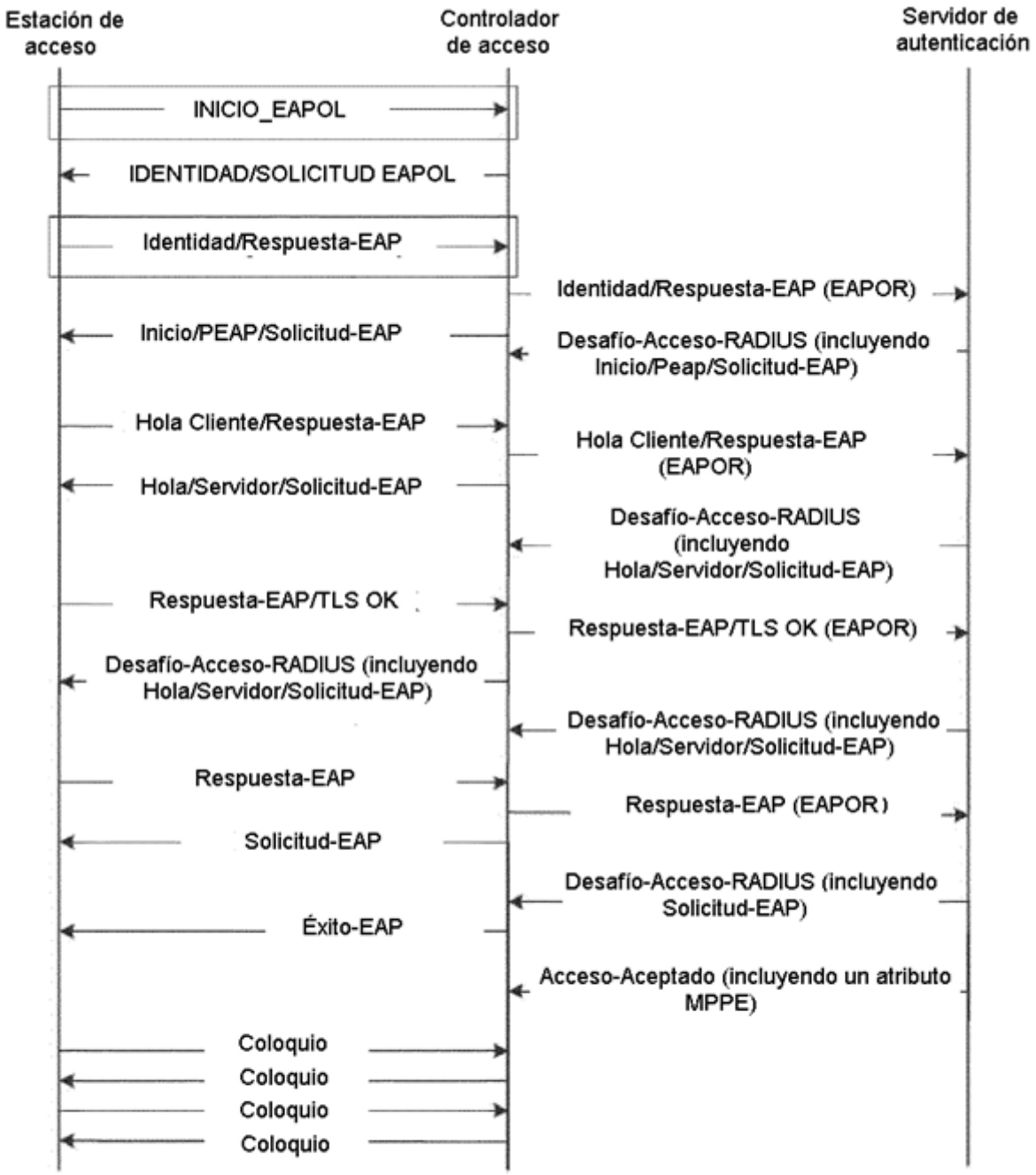
Estación de acceso
Controlador de acceso
Servidor de autenticación
INICIO_EAPOL
IDENTIDAD/SOLICITUD EAPOL
Identidad/Respuesta-EAP
Identidad/Respuesta-EAP (EAPOR)
Inicio/PEAP/Solicitud-EAP
Desafío-Acceso-RADIUS (incluyendo Inicio/Peap/Solicitud-EAP)
Hola Cliente/Respuesta-EAP
Hola Cliente/Respuesta-EAP (EAPOR)
Hola/Servidor/Solicitud-EAP
Desafío-Acceso-RADIUS (incluyendo Hola/Servidor/Solicitud-EAP)
Respuesta-EAP/TLS OK
Respuesta-EAP/TLS OK (EAPOR)
Desafío-Acceso-RADIUS (incluyendo Hola/Servidor/Solicitud-EAP)
Desafío-Acceso-RADIUS (incluyendo Hola/Servidor/Solicitud-EAP)
Respuesta-EAP
Respuesta-EAP (EAPOR)
Solicitud-EAP
Desafío-Acceso-RADIUS (incluyendo Solicitud-EAP)
Éxito-EAP
Acceso-Aceptado (incluyendo un atributo MPPE)
Coloquio
Coloquio
Coloquio
Coloquio

FIG. 3B

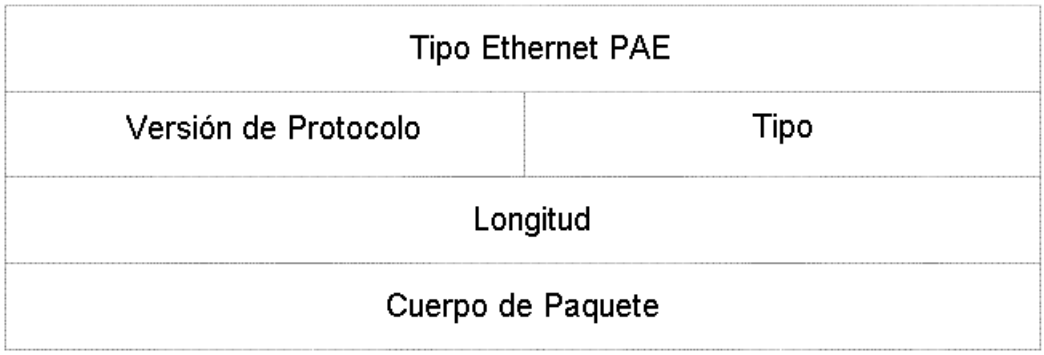

FIG. 3C

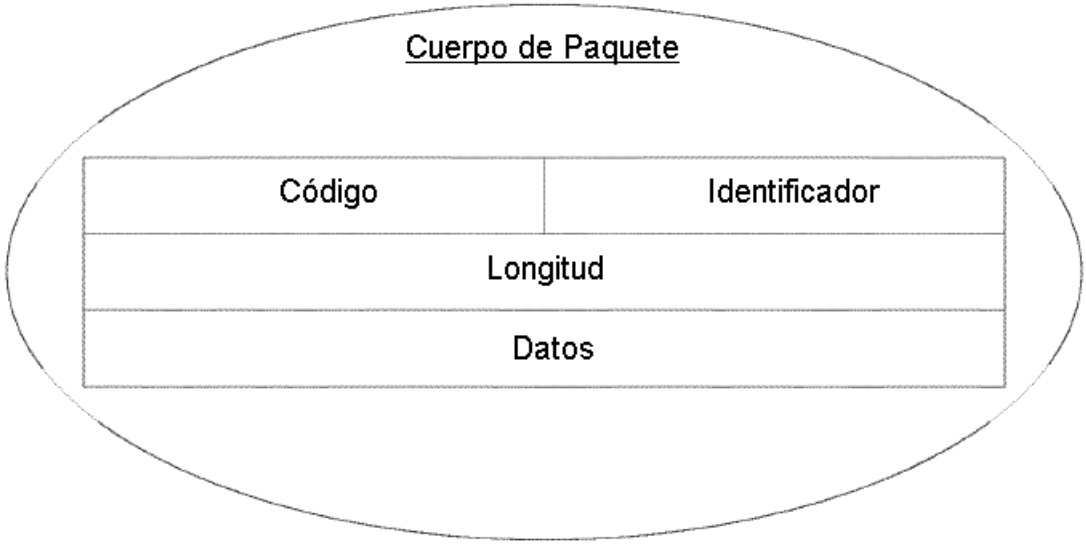

FIG. 3D

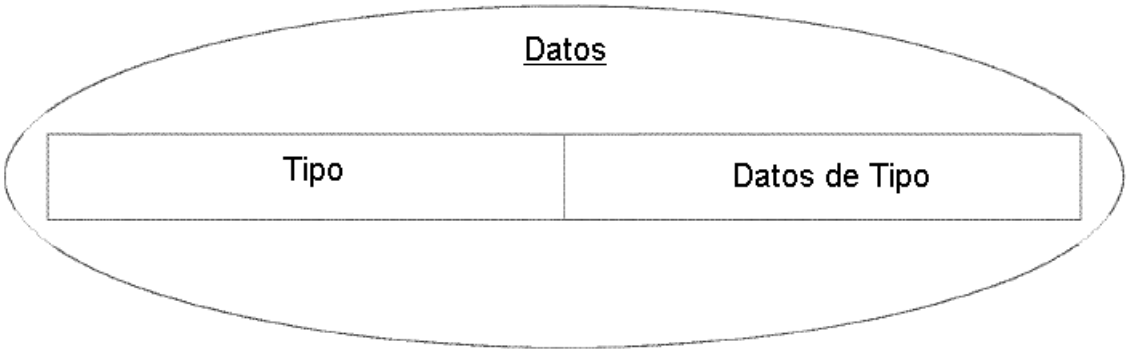

FIG. 3E

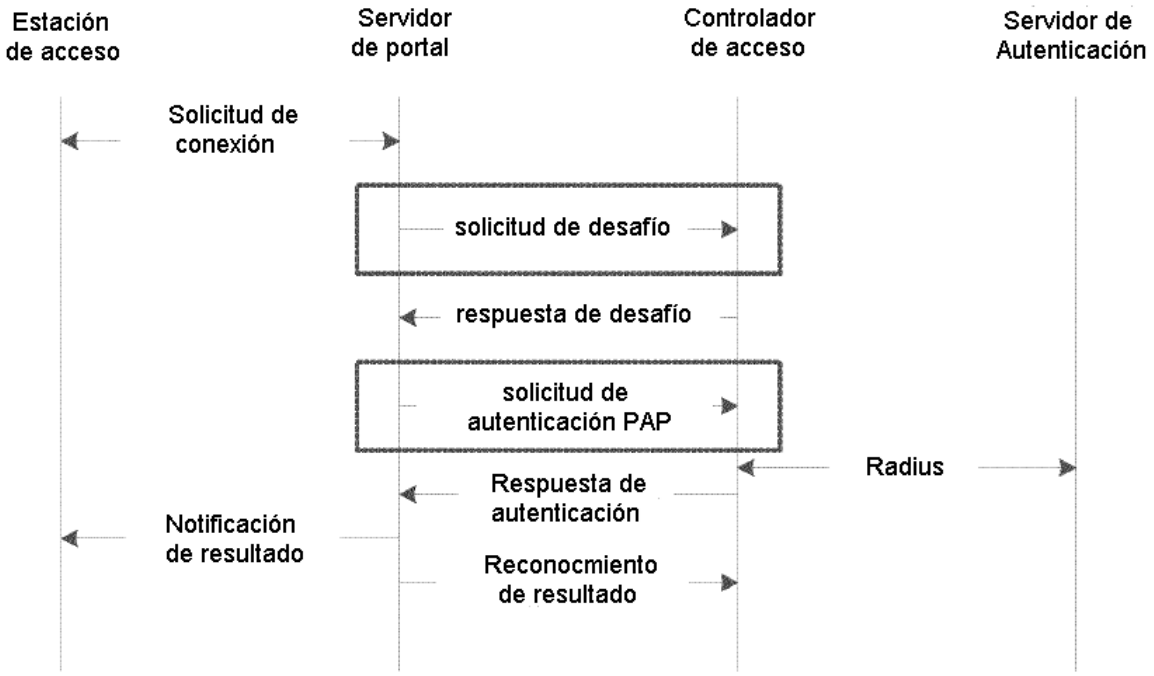
Estación de acceso
Servidor de portal
Controlador de acceso
Servidor de Autenticación
Solicitud de conexión
solicitud de desafío
respuesta de desafío
solicitud de autenticación PAP
Radius
Respuesta de autenticación
Notificación de resultado
Reconocmiento de resultado

FIG. 3F

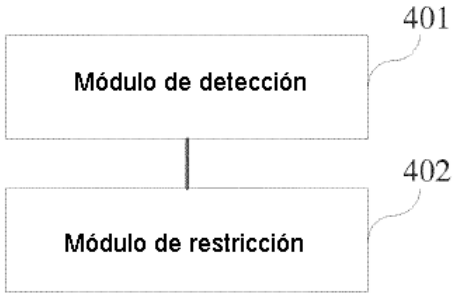
401
Módulo de detección
402
Módulo de restricción

FIG. 4

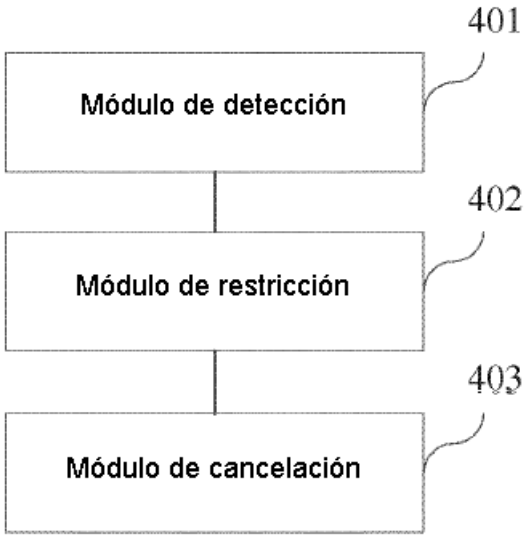
401
Módulo de detección
402
Módulo de restricción
403
Módulo de cancelación

FIG. 5

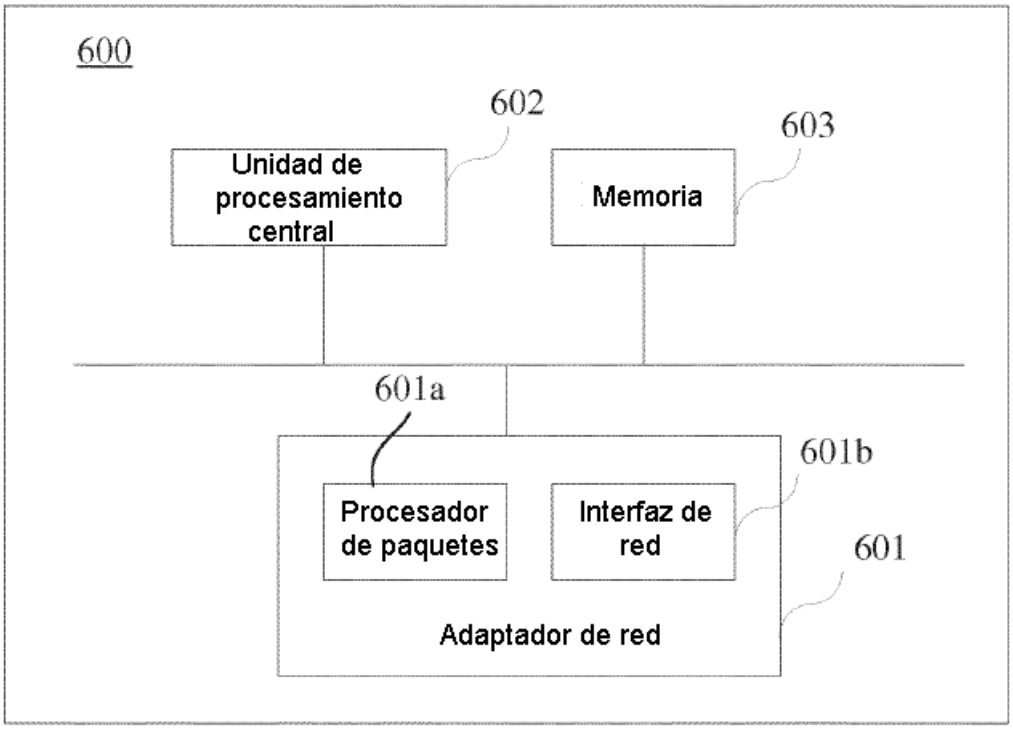
600
602
Unidad de procesamiento central
603
Memoria
601a
601b
Procesador de paquetes
Interfaz de red
601
Adaptador de red

FIG. 6