(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 787 749**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/70 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.10.2016 E 16196618 (9)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2020 EP 3169036**

(54) Título: **Método, aparato y dispositivo de procesamiento de paquetes**

(30) Prioridad:

06.11.2015 CN 201510752291

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.10.2020

(73) Titular/es:

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

(72) Inventor/es:

XU, YIBIN y
SUN, BING

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método, aparato y dispositivo de procesamiento de paquetes

Campo técnico

La presente invención se refiere al campo de las tecnologías de la comunicación y, en particular, a un dispositivo, aparato y método de procesamiento de paquetes.

Antecedentes

En general, la autenticación de usuario puede necesitar completarse en un dispositivo de autenticación antes de que un terminal acceda a una red. El terminal puede acceder a la red (lo cual se hace referencia también como estar en línea) solo después de completar la autenticación de usuario. El terminal también se comunica con el dispositivo de autenticación cuando está en línea y cuando sale de la red accedida por el terminal (lo cual también se refiere como estar fuera de línea).

El terminal o el servidor de autenticación se comunica con el dispositivo de autenticación utilizando un protocolo de acceso. Un protocolo de acceso común utiliza un protocolo de portal (en inglés: portal), el Protocolo Punto a Punto sobre Ethernet (en inglés: Point-to-Point Protocol over Ethernet, PPPoE abreviado) y el protocolo de autenticación extensible sobre una red de área local (en inglés: Extensible Authentication Protocol over local area network, EAPOL abreviado). El protocolo de portal es un protocolo en una solución utilizada cuando un servicio de red de área local está proporcionado por medios de autenticación web (en inglés: web) e incluye el protocolo de autenticación de contraseña (en inglés: Password Authentication Protocol, PAP abreviado) y el Protocolo de autenticación por desafío mutuo (en inglés: Challenge Handshake Authentication Protocol, CHAP abreviado).

En la actualidad, para evitar que una unidad central de procesamiento (en inglés: central processing unit, CPU abreviado) se vea atacada, cuando una velocidad en la que se recibe un paquete de protocolo de acceso alcanza un límite superior preestablecido, el dispositivo de autenticación restringe la velocidad del paquete de protocolo de acceso. Una medida de restricción específica es que un paquete de protocolo de acceso se descarta de manera aleatoria.

Después de que el paquete se descarta aleatoriamente, la calidad de servicio de un proveedor se ve afectada. Como resultado, la experiencia de servicio es deficiente.

El documento US 20070274290 A1 proporciona una tabla 17 de gestión. Cada entrada de tabla incluye una información de control de reenvío de paquetes para cada terminal de usuario, en asociación con los números 171 de puerto del lado del usuario. La información de control de reenvío de paquetes indica la relación entre una dirección 172 de terminal MAC, una ID 173 de sesión y un resultado 174 de autenticación. Un L2GW 10-1 asigna una ID de sesión a una nueva sesión PPP solicitada por la petición de descubrimiento activa PPPOE (PADR, por su sigla en inglés) y agrega una nueva entrada de tabla a la tabla 17 de gestión. Al recibir la trama PPPOE que incluye el paquete de terminación de descubrimiento activa PPPOE (PADT, por su sigla en inglés) que procede del terminal del usuario, el L2GW 10-1 verifica si la dirección de origen MAC (dirección de terminal MAC) de la trama recibida y la ID de sesión se han registrado en la tabla 17 de gestión de usuarios. Si esos elementos se han registrado, el L2GW 10-1 limpia la entrada de tabla que tiene la dirección MAC de origen anterior de la tabla 17 de gestión de usuario. De otro modo, el L2GW 10-1 descarta el paquete recibido.

Compendio

Para resolver un problema de que la experiencia de servicio de usuario sea deficiente debido al descarte aleatorio de un paquete, esta aplicación proporciona un dispositivo, aparato y método de procesamiento de paquetes. La presente invención se define en las reivindicaciones adjuntas.

De acuerdo con un primer aspecto, se proporciona un método de procesamiento de paquetes, donde el método incluye:

recibir, mediante un plano de reenvío, un elemento de un plano de control del plano de reenvío,

donde el elemento incluye un identificador de un terminal conectado;

recibir, por el plano de reenvío, un paquete de protocolo de acceso;

cuando el plano de reenvío determina que el paquete de protocolo de acceso no es un paquete de inicio de autenticación, determinar, por el plano de reenvío según el identificador del terminal conectado, si un terminal servido por el paquete de protocolo de acceso es el terminal conectado, donde el paquete de inicio de autenticación es un paquete de autenticación que se emplea para iniciar un proceso de autenticación para un terminal servido por el paquete de inicio de autenticación; y

descartar, por el plano de reenvío, el paquete de protocolo de acceso cuando el paquete de protocolo de acceso

no es el paquete de inicio de autenticación y el terminal servido por el paquete de protocolo de acceso no es el terminal conectado.

El plano de reenvío puede obtener el identificador del terminal conectado recibiendo el elemento desde el plano de control. Puesto que un paquete de protocolo de acceso que sirve a un terminal a conectar de nuevo puede ser solo un paquete de inicio de autenticación, cuando el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el terminal servido por el paquete de protocolo de acceso no es el terminal conectado, el plano de reenvío puede determinar que el paquete de protocolo de acceso es un paquete de error o un paquete de ataque, y descartar el paquete de protocolo de acceso. En comparación con el descarte aleatorio de un paquete, el presente método no solo reduce la carga de procesamiento en el plano de control, sino que también evita impactos indeseados en un usuario y, por lo tanto, se puede mejorar la experiencia de servicio del usuario.

Haciendo referencia al primer aspecto, en la primera implementación del primer aspecto, el método incluye adicionalmente:

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en una cola de paquetes de un terminal a conectar de nuevo cuando el plano de reenvío determina que el paquete de protocolo de acceso es el paquete de inicio de autenticación; o

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en una cola de paquetes del terminal conectado cuando el plano de reenvío determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el plano de reenvío determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado; y

programar, por el plano de reenvío, la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado según las respectivas prioridades de la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado, donde la prioridad de la cola de paquetes del terminal a conectar de nuevo es distinta de la prioridad de la cola de paquetes del terminal conectado.

La prioridad de la cola de paquetes del terminal a conectar de nuevo y la prioridad de la cola de paquetes del terminal conectado se establece según una necesidad real y, entonces, las colas se programan según las prioridades de las colas, lo cual puede mejorar la experiencia de servicio del usuario. Por ejemplo, la cola de paquetes del terminal conectado puede programarse de manera preferente y, de este modo, se puede procesar un servicio del terminal conectado de manera oportuna.

Haciendo referencia a un primer aspecto o a la primera implementación del primer aspecto, en la segunda implementación del primer aspecto, el elemento incluye adicionalmente un estado de autenticación del terminal conectado, el estado de autenticación se encuentra en autenticación incompleta o en autenticación completada, la cola de paquetes del terminal conectado incluye una cola de paquetes bajo autenticación y una cola de paquetes de autenticación completada, y una prioridad de la cola de paquetes bajo autenticación es distinta a una prioridad de la cola de paquetes de autenticación completada; y

el posicionamiento, por un plano de reenvío, el paquete de protocolo de acceso en una cola de paquetes del terminal conectado incluye:

determinar, por el plano de reenvío, un estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en la cola de paquetes bajo autenticación cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta; o

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en la cola de paquetes de autenticación completada cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada.

Se establecen la cola de paquetes del terminal a conectar de nuevo, la cola de paquetes bajo autenticación y la cola de paquetes de autenticación completada, y la prioridad de la cola de paquetes del terminal a conectar de nuevo, la prioridad de la cola de paquetes bajo autenticación y la prioridad de la cola de paquetes de autenticación completada se establecen según a una necesidad real; por lo tanto, cuando las colas se programan según las prioridades de las colas, se puede mejorar adicionalmente la experiencia de servicio del usuario.

Haciendo referencia a uno cualquiera del primer aspecto, la primera implementación del primer aspecto y la segunda implementación del primer aspecto, en la tercera implementación del primer aspecto, el elemento incluye adicionalmente el estado de autenticación del terminal conectado, y el estado de autenticación se encuentra en autenticación incompleta o en autenticación completada, y el método incluye adicionalmente:

cuando el plano de reenvío determina que el paquete de protocolo de acceso no es el paquete de inicio de

autenticación y el plano de reenvío determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, determinar, por el plano de reenvío, el estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta y cuando el plano de reenvío determina que el paquete de protocolo de acceso es un paquete en línea; o

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada y cuando el plano de reenvío determina que el paquete de protocolo de acceso es un paquete de autenticación distinto al paquete de inicio de autenticación.

Debido a que un paquete de protocolo de acceso de un terminal conectado cuyo estado de autenticación de servicio se encuentra en autenticación completada solo puede ser un paquete de inicio de autenticación, un paquete en línea o un paquete fuera de línea, y un paquete de protocolo de acceso de un terminal conectado cuyo estado de autenticación de servicio se encuentra en autenticación incompleta solo puede ser un paquete de autenticación o un paquete fuera de línea, tanto un paquete de autenticación que es distinto al paquete de inicio de autenticación y que sirve al terminal conectado cuyo estado de autenticación se encuentra en autenticación completada como un paquete en línea que sirve al terminal conectado cuyo estado de autenticación se encuentra en autenticación incompleta sean paquetes de error o paquetes de ataque; después de descartar los paquetes de error o paquetes de ataque, se mejora adicionalmente la experiencia del usuario, y se reduce la carga de procesamiento en el plano de control.

Haciendo referencia a cualquiera uno del primer aspecto, la primera implementación del primer aspecto, la segunda implementación del primer aspecto, y la tercera implementación del primer aspecto, en la cuarta implementación del primer aspecto, el método incluye adicionalmente:

recibir, por el plano de reenvío, una indicación que se envía por el plano de control, donde la indicación se emplea para indicar que una cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a una cantidad preestablecida; y limitar, por el plano de reenvío, una velocidad a la que se envía el paquete de inicio de autenticación al plano de control.

Cuando la cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a la cantidad preestablecida, indica que la carga de procesamiento en el plano de control es grave. En este caso, el plano de reenvío restringe la velocidad a la que el paquete de inicio de autenticación se envía al plano de control, lo cual puede reducir la carga de procesamiento del plano de control.

De acuerdo con un segundo aspecto, se proporciona un aparato de procesamiento de paquetes, donde el aparato incluye varias unidades, tales como una unidad de recepción y una unidad de procesamiento, y las varias unidades están configuradas para implementar el método proporcionado en el primer aspecto.

De acuerdo con un tercer aspecto, se proporciona un dispositivo de procesamiento de paquetes, donde el dispositivo incluye un aparato de plano de control y un aparato de plano de reenvío, donde

el aparato de plano de control está configurado para enviar un elemento al aparato de plano de reenvío, donde el elemento incluye un identificador de un terminal conectado; y

el aparato de plano de reenvío incluye al menos una memoria, un procesador y una interfaz de comunicación, donde la memoria está configurada para almacenar una instrucción; el procesador está configurado para ejecutar la instrucción almacenada en la memoria; la interfaz de comunicación está configurada para comunicarse con el aparato de plano de control bajo el control del procesador; y el procesador puede implementar, ejecutando la instrucción almacenada en la memoria, el método proporcionado en el primer aspecto.

De acuerdo con un cuarto aspecto, se proporciona un medio de almacenamiento legible por ordenador, donde el medio de almacenamiento legible por ordenador está configurado para almacenar el código del programa que se ejecuta por el anterior aparato de plano de reenvío cuando el anterior aparato de plano de reenvío procesa un paquete, y el código del programa incluye una instrucción empleada para implementar el método proporcionado en el primer aspecto.

Breve descripción de los dibujos

Para describir las soluciones técnicas en las realizaciones de la presente invención más claramente, lo que sigue describe brevemente los dibujos adjuntos necesarios para describir las realizaciones. Aparentemente, los dibujos adjuntos en la siguiente descripción muestran meramente algunas realizaciones de la presente invención, y una persona con experiencia ordinaria en la técnica puede aún obtener otros dibujos a partir de estos dibujos adjuntos sin ningún esfuerzo creativo.

La FIG. 1 es un diagrama esquemático de una arquitectura de red de un sistema de autenticación según una realización de la presente invención;

la FIG. 2 es un diagrama estructural esquemático de un dispositivo de autenticación según una realización de la

presente invención;

la FIG. 3 es un diagrama de flujo de un método de procesamiento de paquetes según una realización de la presente invención; y

la FIG. 4 es un diagrama esquemático de un formato de un paquete EAPOL según una realización de la presente invención.

Descripción de realizaciones

Para hacer los objetivos, soluciones técnicas y ventajas de la presenta invención de forma más clara, lo siguiente describe modos de implementación de la presente invención en detalle haciendo referencia a los dibujos adjuntos.

Para facilitar la comprensión de las soluciones técnicas proporcionadas en las realizaciones de la presente invención, se describe, en primer lugar, una arquitectura de red de un sistema de autenticación haciendo referencia a la FIG. 1. Tal como se muestra en la FIG. 1, un dispositivo de red de una arquitectura de red incluye al menos un terminal, un dispositivo de autenticación y un servidor de autenticación. El dispositivo de autenticación es un dispositivo de red que procesa un paquete de protocolo de acceso entre el terminal y el servidor de autenticación. Por ejemplo, el dispositivo de autenticación puede ser un enrutador o un conmutador de red. El paquete de protocolo de acceso puede ser uno cualquiera de un paquete de protocolo de portal, un paquete de protocolo de PPPoE o un paquete EAPOL.

Si el paquete de protocolo de acceso es un paquete EAPOL, el terminal se comunica con el dispositivo de autenticación utilizando el paquete EAPOL, y el dispositivo de autenticación se comunica con el servidor de autenticación utilizando el protocolo de servicio de autenticación remota de llamadas de usuarios (en inglés: Remote Authentication Dial-In User Service, RADIUS abreviado).

Si el paquete de protocolo de acceso es un paquete de protocolo de portal, el dispositivo de red de la arquitectura de red incluye adicionalmente un servidor de portal. El servidor de portal está conectado tanto al dispositivo de autenticación como al terminal. Por ejemplo, el servidor de portal puede ser un ordenador personal o puede ser un servidor de aplicación web (en inglés: web); y el servidor de portal tiene software de autenticación de portal cautivo (en inglés: portal cautivo). El terminal se comunica con el servidor de portal utilizando el Protocolo de Transferencia de hipertexto (en inglés: Hypertext Transfer Protocol, HTTP abreviado), y el dispositivo de autenticación se comunica con el servidor del portal empleando un protocolo de portal.

La FIG. 2 es un diagrama esquemático de una posible estructura de soporte físico del dispositivo de autenticación que se muestra en la FIG. 1. Tal como se muestra en la FIG. 2, el dispositivo de autenticación incluye un aparato 10 de plano de control y un aparato 20 de plano de reenvío. El aparato 10 de plano de control puede ser un chip de control. Por ejemplo, el aparato 10 de plano de control puede implementarse por un CPU, o puede implementarse por un procesador de red (en inglés: network processor, NP abreviado) con una función de plano de control. El aparato 20 de plano de reenvío puede ser un chip de conmutación. Por ejemplo, el aparato 20 de plano de reenvío puede implementarse por un circuito integrado específico de aplicación (en inglés: application-specific integrated circuit, ASIC abreviado), un dispositivo lógico programable (en inglés: programmable logic device, PLD abreviado), un NP, un núcleo que se encuentra en un CPU multinúcleo y que se utiliza para implementar un plano de reenvío, o cualquier combinación de los mismos. El PLD puede ser un dispositivo lógico programable complejo (en inglés: complex programmable logic device, CPLD abreviado), una disposición de puertos programables de campo (en inglés: field-programmable gate array, FPGA abreviado), una matriz lógica genérica (en inglés: generic array logic, GAL abreviado), o cualquier combinación de los mismos.

El aparato 20 de plano de reenvío está configurado para implementar el plano de reenvío del dispositivo de autenticación. Un paquete de protocolo de acceso recibido por el dispositivo de autenticación se procesa, en primer lugar, por el aparato 20 de plano de reenvío. El aparato 20 de plano de reenvío determina si enviar o no el paquete de protocolo de acceso al aparato 10 de plano de control. El aparato 20 de plano de reenvío mantiene una tabla de estado del terminal de acuerdo con un elemento que se envía por el aparato 10 de plano de control. Una entrada de la tabla de estado del terminal incluye un identificador de un terminal conectado en el elemento que se envía por el aparato 10 de plano de control. El aparato 10 de plano de control puede enviar múltiples elementos. También pueden existir identificadores de múltiples terminales conectados en el elemento que se envía por el aparato 10 de plano de control. En consecuencia, una única entrada de la tabla de estado del terminal puede almacenar los identificadores de los múltiples terminales conectados, o la tabla de estado del terminal puede incluir múltiples entradas, y cada entrada almacena un identificador de un terminal conectado. El terminal conectado se refiere a un terminal para el cual se ha iniciado un proceso de autenticación, pero no se ha completado la autenticación, o un terminal que se ha autenticado y está en línea. El aparato 20 de plano de reenvío determina, en primer lugar, si el paquete de protocolo de acceso es un paquete de inicio de autenticación o no. El paquete de inicio de autenticación se refiere a un paquete de autenticación que se utiliza para iniciar un proceso de autenticación para un terminal servido por el paquete de inicio de autenticación. Un terminal servido por el paquete de protocolo de acceso se refiere a un terminal el que pertenece un proceso de autenticación que implica al paquete de protocolo de acceso. Por ejemplo, un paquete de protocolo que se envía por un terminal para autenticar el terminal es un paquete de protocolo de acceso que sirve al terminal. Para otro ejemplo, el paquete de protocolo de acceso que indica un resultado de autenticación de un terminal y que se

envía por un servidor es un paquete de protocolo de acceso que sirve al terminal. Si el paquete de protocolo de acceso es el paquete de inicio de autenticación, el aparato 20 de plano de reenvío envía el paquete de protocolo de acceso 10 al aparato de plano de control. Opcionalmente, el aparato 20 de plano de reenvío posiciona el paquete de protocolo de acceso en una cola de paquetes, y envía el paquete de protocolo de acceso al aparato 10 de plano de control después de la programación de la cola. La cola de paquetes se utiliza para almacenar un paquete que se envía por el aparato 20 de plano de reenvío al aparato 10 de plano de control. Si el paquete de protocolo de acceso no es el paquete de inicio de autenticación, el aparato 20 de plano de reenvío busca la tabla de estado del terminal para una entrada que coincide con el paquete de protocolo de acceso. Cuando el aparato 20 de plano de reenvío no encuentra la entrada que coincide con el paquete de protocolo de acceso, el aparato 20 de plano de reenvío descarta el paquete de protocolo de acceso recibido. Cuando el aparato 20 de plano de reenvío encuentra la entrada que coincide con el paquete de protocolo de acceso, el aparato 20 de plano de reenvío envía el paquete de protocolo de acceso al aparato 10 de plano de control. Opcionalmente, el aparato 20 de plano de reenvío posiciona el paquete de protocolo de acceso en una cola de paquetes, y envía el paquete de protocolo de acceso al aparato 10 de plano de control después de la programación de la cola. Después de recibir el paquete de protocolo de acceso que se envía por el aparato 20 de plano de reenvío, el aparato 10 de plano de control procesa el paquete de protocolo de acceso según un protocolo de acceso correspondiente. Si el paquete de protocolo de acceso es el paquete de inicio de autenticación, después de que el aparato 10 de plano de control procese el paquete de protocolo de acceso, el terminal servido por el paquete de protocolo de acceso se convierte en un terminal conectado. El aparato 10 de plano de control envía un elemento que incluye un identificador del terminal conectado al aparato 20 de plano de reenvío.

El dispositivo de autenticación que se muestra en la FIG. 2 tiene tanto el aparato de plano de reenvío como el aparato de plano de control. En otra estructura de soporte físico posible, se puede implementar un plano de control por un dispositivo independiente. Por ejemplo, en redes definidas por software, el plano de control puede implementarse por un controlador. El controlador puede controlar el aparato de plano de reenvío empleando un protocolo (tal como el protocolo OpenFlow) que soporta las redes definidas por software. En este caso, una combinación de un dispositivo que implementa independientemente el aparato de plano de reenvío y un dispositivo que implementa independientemente el aparato de plano de control también puede considerarse como el dispositivo de autenticación.

En esta realización de la presente invención, el paquete de protocolo de acceso puede clasificarse en un paquete de autenticación, un paquete en línea, o un paquete fuera de línea. El paquete de autenticación es un paquete que se envía por un terminal o un servidor (por ejemplo, un servidor de portal) a un dispositivo de autenticación en un proceso de autenticación. El paquete de autenticación puede ser el paquete de inicio de autenticación, o puede ser un paquete de autenticación distinto del paquete de inicio de autenticación. El paquete en línea y el paquete fuera de línea son paquetes que se envían por un terminal o un servidor a un dispositivo de autenticación en un proceso en línea después de completar la autenticación. Una diferencia entre el paquete en línea y el paquete fuera de línea reside en que: el paquete fuera de línea se emplea para implementar el estar fuera de línea del terminal, mientras que el paquete en línea se emplea para implementar un servicio en línea del terminal (por ejemplo, utilizado para consultar el tráfico del terminal).

La FIG. 3 es un diagrama de flujo de un método de procesamiento de paquetes según una realización de la presente invención. Tal como se muestra en la FIG. 3, el método incluye las siguientes etapas:

Etapa 301. Un plano de reenvío recibe un elemento que procede de un plano de control.

El plano de reenvío puede implementarse por el aparato de plano de reenvío del dispositivo de autenticación que se muestra en la FIG. 2. El plano de control puede implementarse por el aparato de plano de control del dispositivo de autenticación que se muestra en la FIG. 2.

El elemento incluye un identificador de un terminal conectado. El identificador del terminal conectado puede ser una dirección de Control de Acceso de Medios (en inglés: Media Access Control, MAC abreviado) o una dirección de Protocolo de Internet (en inglés: Internet Protocol, IP abreviado) del terminal conectado.

Opcionalmente, el elemento que se envía por el plano de control incluye adicionalmente un estado de autenticación del terminal conectado, donde el estado de autenticación se encuentra en autenticación incompleta o en autenticación completada.

Después de recibir el elemento, el plano de reenvío almacena el identificador y el estado de autenticación del terminal conectado que se incluyen en el elemento a una tabla de estado del terminal. Específicamente, la tabla de estado del terminal incluye varias entradas, y el identificador y el estado de autenticación del terminal conectado se registran en las entradas.

Cuando el plano de control recibe un paquete de inicio de autenticación, si se determina que un estado de autenticación de un terminal servido por el paquete de inicio de autenticación se encuentra en autenticación incompleta, el estado de autenticación del terminal conectado en el elemento que se envía por el plano de control al plano de reenvío se encuentra en autenticación incompleta. Si un proceso de autenticación se encuentra completado para el terminal conectado posteriormente, el plano de control actualiza el estado de autenticación del terminal conectado a autenticación completada y, a continuación, envía al plano de reenvío, un elemento en el que se actualiza el estado

de autenticación, donde el estado de autenticación del terminal conectado en el elemento se encuentra en autenticación completada. Además, si el terminal conectado reinicia el proceso de autenticación posteriormente, el plano de control actualiza el estado de autenticación del terminal conectado a autenticación incompleta y, a continuación, envía al plano de reenvío, un elemento en el que se actualiza el estado de autenticación, donde el estado de autenticación del terminal conectado en el elemento se encuentra en autenticación incompleta.

Opcionalmente, el plano de control también controla en tiempo real una cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta. Cuando la cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a una cantidad preestablecida, el plano de control envía una indicación al plano de reenvío, donde la indicación se emplea para indicar que la cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a la cantidad preestablecida. Sobre esta premisa, la etapa 301 puede incluir adicionalmente: el plano de reenvío recibe la indicación que se envía por el plano de control.

En su implementación, la cantidad preestablecida puede calcularse según un parámetro de rendimiento del plano de control. Si la cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a la cantidad preestablecida, la carga en el plano de control alcanza o se encuentra cerca de un límite superior de capacidad de procesamiento.

Opcionalmente, cuando la cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta disminuye a un intervalo preestablecido, el plano de control envía otra indicación al plano de reenvío, donde la otra indicación se emplea para indicar que la cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta disminuye al intervalo preestablecido.

La etapa 301 incluye adicionalmente: el plano de reenvío recibe la otra indicación que se envía por el plano de control. En su implementación, un límite superior del intervalo preestablecido puede ser la cantidad preestablecida anterior o puede establecerse a un valor inferior a la cantidad preestablecida anterior.

Etapa 302. El plano de reenvío recibe un paquete de protocolo de acceso.

Opcionalmente, después de que el plano de reenvío recibe la indicación que se envía por el plano de control, la etapa 302 incluye adicionalmente: el plano de reenvío limita una velocidad a la que se envía un paquete de inicio de autenticación al plano de control.

Cuando se va a realizar una limitación en la velocidad a la que se envía el paquete de inicio de autenticación al plano de control, se puede limitar una cantidad o un volumen de datos de paquetes de inicio de autenticación que se envían al plano de control por unidad de tiempo.

Cuando la cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a la cantidad preestablecida, indica que la carga en el plano de control alcanza o se encuentra cerca del límite superior de capacidad de procesamiento. En este caso, el plano de reenvío limita la velocidad a la que se envía el paquete de inicio de autenticación al plano de control, de modo que se controla un aumento de la carga de procesamiento en el plano de control, y el plano de control puede procesar un proceso en línea del terminal conectado.

Opcionalmente, después de que el plano de reenvío recibe la otra indicación que se envía por el plano de control, la etapa 302 incluye adicionalmente: cancelar la limitación en la velocidad a la que se envía el paquete de inicio de autenticación al plano de control.

Etapa 303. El plano de reenvío determina si el paquete de protocolo de acceso recibido es un paquete de inicio de autenticación o no.

Cuando el paquete de protocolo de acceso recibido no es el paquete de inicio de autenticación, se realiza la etapa 304. Cuando el paquete de protocolo de acceso recibido es el paquete de inicio de autenticación, se realiza la etapa 306.

Opcionalmente, el paquete de protocolo de acceso incluye un campo que se utiliza para indicar un tipo del paquete de protocolo de acceso. El plano de reenvío puede identificar el tipo del paquete de protocolo de acceso según el campo, para determinar si el paquete de protocolo de acceso es el paquete de inicio de autenticación. El tipo del paquete de protocolo de acceso incluye un paquete de inicio de autenticación, un paquete de autenticación distinto del paquete de inicio de autenticación, un paquete en línea y un paquete fuera de línea. La FIG. 4 muestra un formato de un paquete EAPOL. En el paquete EAPOL, tal como se muestra en la FIG. 4, un campo de tipo (en inglés: type) de Ethernet (en inglés: Ethernet) de Entidad de Acceso de Puerto (en inglés: Port Access Entity, PAE abreviado) representa un tipo de protocolo; un campo de versión de protocolo (en inglés: protocol version) representa un número de versión de protocolo que es admitido por un emisor del paquete EAPOL; se emplea un campo de cuerpo de paquete (en inglés: packet body) para portar una trama de datos del paquete EAPOL; un campo de tipo (en inglés: type) representa un tipo de la trama de datos; y un campo de longitud (en inglés: length) representa una longitud de datos, es decir, una longitud del campo de cuerpo de trama de datos. Los valores del campo de tipo indican distintos tipos de tramas de datos. El campo de tipo puede utilizarse para indicar el tipo del paquete de protocolo de acceso. Por

ejemplo, cuando un valor del campo de tipo del paquete EAPOL es 1 (o se representa como 0x01), el tipo de la trama de datos es una trama de inicio (en inglés: Start) de autenticación, donde un tipo indicado del paquete EAPOL es un paquete de inicio de autenticación.

Etapa 304. El plano de reenvío determina, según un identificador de un terminal conectado, si un terminal servido por el paquete de protocolo de acceso es o no el terminal conectado.

Cuando se determina que el terminal servido por el paquete de protocolo de acceso no es el terminal conectado, es decir, cuando el terminal servido por el paquete de protocolo de acceso es un terminal a conectar de nuevo, se realiza la etapa 305. Cuando se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, se realiza la etapa 306.

Opcionalmente, el plano de reenvío determina, según un protocolo de acceso al cual pertenece el paquete de protocolo de acceso, el terminal servido por el paquete de protocolo de acceso. Por ejemplo, cuando el paquete de protocolo de acceso recibido es un paquete EAPOL, un identificador del terminal servido por el paquete de protocolo de acceso es una dirección MAC de origen del paquete EAPOL. Cuando el paquete de protocolo de acceso recibido es un paquete de protocolo de portal, un identificador del terminal servido por el paquete de protocolo de acceso es una dirección IP, incluido en el paquete de protocolo de portal, del terminal servido por el paquete de protocolo de acceso.

Opcionalmente, el plano de reenvío realiza coincidencias, en una entrada de la tabla de estado del terminal, con el identificador del terminal servido por el paquete de protocolo de acceso. Si el identificador del terminal servido por el paquete de protocolo de acceso se encuentra haciéndolo coincidir en la entrada, se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado. Si el identificador del terminal servido por el paquete de protocolo de acceso no se encuentra haciéndolo coincidir en la entrada, se determina que el terminal servido por el paquete de protocolo de acceso no es el terminal conectado.

Etapa 305. El plano de reenvío descarta el paquete de protocolo de acceso.

En general, un paquete de protocolo de acceso que se envía por un terminal o un servidor al dispositivo de autenticación es un paquete normal, tal como el paquete de inicio de autenticación que se envía por el terminal a conectar de nuevo al dispositivo de autenticación, o un paquete fuera de línea que se envía por el terminal conectado al dispositivo de autenticación. Si el terminal o el servidor tiene un error, o el dispositivo de autenticación se ve atacado, el paquete de protocolo de acceso recibido por el dispositivo de autenticación puede ser un paquete de error o un paquete de ataque. Por ejemplo, el paquete de error o el paquete de ataque pueden ser un paquete en línea o un paquete fuera de línea que sirve al terminal a conectar de nuevo. En una tecnología convencional, un plano de reenvío no diferencia un terminal servido por un paquete de protocolo de acceso y un tipo del paquete de protocolo de acceso, sino que envía todos los paquetes de protocolo de acceso recibidos a un plano de control para su procesamiento. Si hay suficientes paquetes de error o paquetes de ataque, una capacidad de procesamiento del plano de control se puede encontrar completamente ocupado. En esta realización de la presente invención, cuando el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el terminal servido por el paquete de protocolo de acceso es el terminal a conectar de nuevo, el plano de reenvío determina que el paquete de protocolo de acceso es un paquete de ataque o un paquete de error, y descarta el paquete de protocolo de acceso, lo cual no solo puede mejorar la experiencia del usuario, sino que también puede reducir la carga de procesamiento en el plano de control.

Etapa 306. El aplano de reenvío envía el paquete de protocolo de acceso al plano de control.

Opcionalmente, el plano de reenvío puede enviar el paquete de protocolo de acceso al plano de control de acuerdo con una secuencia en la que se reciben los paquetes de protocolo de acceso, es decir, en primer lugar, enviar un paquete de protocolo de acceso que se recibe primero y, a continuación, enviar un paquete de protocolo de acceso que se recibe después. Por ejemplo, el plano de reenvío puede posicionar el paquete de protocolo de acceso en una cola de paquetes, y la cola de paquetes es una cola de tipo primeras entradas, primeras salidas (en inglés: first-in, first-out, FIFO abreviado). Después de programar la cola, el plano de reenvío envía el paquete de protocolo de acceso al plano de control.

Opcionalmente, cuando el plano de reenvío determina que el paquete de protocolo de acceso es el paquete de inicio de autenticación, el plano de reenvío posiciona el paquete de protocolo de acceso en una cola de paquetes del terminal a conectar de nuevo. Cuando el plano de reenvío determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, el plano de reenvío sitúa el paquete de protocolo de acceso en una cola de paquetes del terminal conectado. El plano de reenvío entonces programa la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado de acuerdo con las respectivas prioridades de la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado. La prioridad de la cola de paquetes del terminal a conectar de nuevo es distinta de la prioridad de la cola de paquetes del terminal conectado.

Opcionalmente, la prioridad de la cola de paquetes del terminal a conectar de nuevo es inferior a la prioridad de la cola de paquetes del terminal conectado. Si hay una pequeña cantidad de paquetes de protocolo de acceso a enviar por el plano de reenvío al plano de control, tanto el paquete de protocolo de acceso en la cola de paquetes del terminal a conectar de nuevo como un paquete de protocolo de acceso en la cola de paquetes del terminal conectado pueden

enviarse sin problemas al plano de control. Si hay una gran cantidad de paquetes de protocolo de acceso a enviar por el plano de reenvío al plano de control, el plano de reenvío programa paquetes en múltiples colas según las prioridades de las colas, y el paquete de protocolo de acceso en la cola de paquetes del terminal conectado se envía al plano de control de manera preferente. Si la cola de paquetes del terminal a conectar de nuevo está completamente ocupada, el paquete de protocolo de acceso en la cola de paquetes del terminal a conectar de nuevo o un paquete de protocolo de acceso que se va a posicionar en la cola de paquetes del terminal a conectar de nuevo puede descartarse.

En su implementación, la prioridad de la cola de paquetes del terminal a conectar de nuevo y la prioridad de la cola de paquetes del terminal conectado se puede establecer según la necesidad real y, entonces, las colas se programan según las prioridades de las colas, lo cual puede mejorar la experiencia de servicio del usuario. Por ejemplo, la cola de paquetes del terminal conectado puede programarse de manera preferente y, de este modo, se puede procesar un servicio del terminal conectado de manera oportuna.

Opcionalmente, la cola de paquetes del terminal conectado incluye una cola de paquetes bajo autenticación y una cola de paquetes de autenticación completada. Una prioridad de la cola de paquetes bajo autenticación es distinta de una prioridad de la cola de paquetes de autenticación completada.

Que el plano de reenvío posicione el paquete de protocolo de acceso recibido en la cola de paquetes del terminal conectado puede incluir específicamente: el plano de reenvío determina un estado de autenticación del terminal servido por el paquete de protocolo de acceso; y cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta, el plano de reenvío posiciona el paquete de protocolo de acceso en una cola de paquetes bajo autenticación; o cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada, el plano de reenvío posiciona el paquete de protocolo de acceso en la cola de paquetes de autenticación completada.

En general, cuando no está completada la autenticación en un terminal, un paquete normal que se envía por el terminal o un servidor al dispositivo de autenticación es un paquete de autenticación distinto a un paquete de inicio de autenticación o un paquete fuera de línea. Después de completar la autenticación en el terminal, un paquete normal que se envía por el terminal o el servidor al dispositivo de autenticación es un paquete en línea o un paquete fuera de línea. Si el terminal o el servidor tiene un error, o el dispositivo de autenticación se ve atacado, un paquete de protocolo de acceso recibido por el dispositivo de autenticación puede ser un paquete de error o un paquete de ataque. Por ejemplo, el paquete de error o el paquete de ataque pueden ser un paquete en línea que sirve al terminal en el que la autenticación no está completada. El paquete de error o el paquete de ataque también pueden ser un paquete de autenticación que es distinto a un paquete de inicio de autenticación y que sirve al terminal en el que la autenticación se ha completado. Opcionalmente, el plano de reenvío puede descartar este tipo de paquete, lo cual mejora adicionalmente la experiencia del usuario y reduce la carga de procesamiento en un plano de control.

Por ejemplo, cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta, el plano de reenvío determina si el paquete de protocolo de acceso es un paquete de autenticación distinto al paquete de inicio de autenticación o a un paquete fuera de línea. Cuando el paquete de protocolo de acceso es un paquete en línea, el paquete de protocolo de acceso se descarta. Cuando el paquete de protocolo de acceso es un paquete de autenticación distinto al paquete de inicio de autenticación o un paquete fuera de línea, el plano de reenvío posiciona el paquete de protocolo de acceso en la cola de paquetes bajo autenticación. Cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada, el plano de reenvío determina si el paquete de protocolo de acceso es un paquete en línea o a un paquete fuera de línea. Cuando el paquete de protocolo de acceso es un paquete de autenticación distinta al paquete de inicio de autenticación, el paquete de protocolo de acceso se descarta. Cuando el paquete de protocolo de acceso es un paquete en línea o un paquete fuera de línea, el plano de reenvío posiciona el paquete de protocolo de acceso en la cola de paquetes de autenticación completada.

Opcionalmente, la prioridad de la cola de paquetes del terminal a conectar de nuevo, la prioridad de la cola de paquetes bajo autenticación y la prioridad de la cola de paquetes de autenticación completada es en orden ascendente. Específicamente, cuando hay paquetes en la cola de paquetes del terminal a conectar de nuevo, la cola de paquetes bajo autenticación y la cola de paquetes de autenticación completada, el plano de reenvío envía preferentemente paquetes en la cola de paquetes de autenticación completada al plano de control hasta que se hayan enviado todos los paquetes en la cola de paquetes de autenticación completada y, a continuación, el plano de reenvío envía los paquetes en la cola de paquetes bajo autenticación al plano de control. El plano de reenvío envía paquetes en la cola de paquetes del terminal a conectar de nuevo al plano de control solo después de que todos los paquetes en la cola de paquetes de autenticación completada y la cola de paquetes bajo autenticación hayan sido enviados. Si hay una pequeña cantidad de paquetes de protocolo de acceso a enviar por el plano de reenvío al plano de control, los paquetes de protocolo de acceso en la cola de paquetes del terminal a conectar de nuevo, la cola de paquetes bajo autenticación y la cola de paquetes de autenticación completada pueden todos enviarse sin problemas al plano de control. Si hay una gran cantidad de paquetes de protocolo de acceso a enviar por el plano de reenvío al plano de control, el paquete de protocolo de acceso en la cola de paquetes de autenticación completada se envía preferentemente al plano de control. Si la cola de paquetes bajo autenticación está completamente ocupada, el paquete de protocolo de acceso en la cola de paquetes bajo autenticación o un paquete de protocolo de acceso que se va a posicionar en la cola de paquetes bajo autenticación se puede descartar. De igual modo, si la cola de paquetes

del terminal a conectar de nuevo está completamente ocupada, el paquete de protocolo de acceso en la cola de paquetes del terminal a conectar de nuevo o un paquete de protocolo de acceso que se va a posicionar en la cola de paquetes del terminal a conectar de nuevo puede descartarse.

Se establece la cola de paquetes del terminal a conectar de nuevo, la cola de paquetes bajo autenticación y la cola de paquetes de autenticación completada, y la prioridad de la cola de paquetes del terminal a conectar de nuevo, la prioridad de la cola de paquetes bajo autenticación y la prioridad de la cola de paquetes de autenticación completada se establecen según una necesidad real; por lo tanto, cuando las colas se programan según las prioridades de las colas, se puede mejorar adicionalmente la experiencia de servicio del usuario.

En esta realización de la presente invención, un plano de reenvío puede obtener un identificador de un terminal conectado recibiendo un elemento que procede de un plano de control; el plano de reenvío recibe un paquete de protocolo de acceso; cuando el plano de reenvío determina que el paquete de protocolo de acceso no es un paquete de inicio de autenticación, el plano de reenvío determina, según el identificador del terminal conectado, si un terminal servido por el paquete de protocolo de acceso recibido es el terminal conectado o no; cuando el terminal servido por el paquete de protocolo de acceso no es el terminal conectado, el paquete de protocolo de acceso se descarta. Puesto que un paquete de protocolo de acceso que sirve a un terminal a conectar de nuevo puede ser solo el paquete de inicio de autenticación, cuando el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el terminal servido por el paquete de protocolo de acceso no es el terminal conectado, es decir, el terminal servido por el paquete de protocolo de acceso es el terminal a conectar de nuevo, se determina que el paquete de protocolo de acceso es un paquete de error o un paquete de ataque, y el paquete de protocolo de acceso se descarta. En comparación con el descarte aleatorio de un paquete, el presente método no solo reduce la carga de procesamiento en el plano de control, sino que también evita impactos indeseados en un usuario y, por lo tanto, se puede mejorar la experiencia de servicio del usuario.

Cabe destacar que cuando el aparato de procesamiento de paquetes proporcionado en la realización anterior procesa un paquete, se emplea la división de los anteriores módulos funcionales como ejemplo ilustrativo. En su aplicación real, las anteriores funciones se pueden ubicar en distintos módulos funcionales e implementarse según una necesidad, es decir, una estructura interna de un dispositivo está dividida en distintos módulos funcionales para implementar todas o partes de las funciones descritas anteriormente. Además, el aparato de procesamiento de paquetes proporcionado en la anterior realización y la realización del método de procesamiento de paquetes pertenecen a la misma idea, y para un proceso de implementación específico del mismo, se puede hacer referencia a la realización del método, y los detalles no se describen en el presente documento.

Una persona con experiencia ordinaria en la técnica puede comprender que todas o algunas de las etapas de las realizaciones pueden implementarse mediante soporte físico o un programa que da instrucciones a un soporte físico relacionado. El programa puede almacenarse en un medio de almacenamiento legible por ordenador. El medio de almacenamiento puede incluir: una memoria de solo lectura, un disco magnético o un disco óptico. Esta realización no es una realización de la invención, aunque resulta de ayuda para comprender determinado aspecto de la misma.

Las anteriores descripciones son meramente realizaciones específicas de la presente invención, aunque no están concebidas para limitar el 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 método de procesamiento de paquetes, en donde el método comprende:

recibir (301), por un plano de reenvío, un elemento que procede de un plano de control del plano de reenvío, en donde el elemento comprende un identificador de un terminal conectado;

recibir (302), por el plano de reenvío, un paquete de protocolo de acceso;

cuando el plano de reenvío determina que el paquete de protocolo de acceso no es un paquete de inicio de autenticación, determinar (304), por el plano de reenvío según el identificador del terminal conectado, si un terminal servido por el paquete de protocolo de acceso es el terminal conectado, en donde el paquete de inicio de autenticación es un paquete de autenticación que se emplea para iniciar un proceso de autenticación para un terminal servido por un paquete de inicio de autenticación; y

descartar (305), por el plano de reenvío, el paquete de protocolo de acceso cuando el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el terminal servido por el paquete de protocolo de acceso no es el terminal conectado.

2. El método de acuerdo con la reivindicación 1, en donde el método comprende adicionalmente:

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en una cola de paquetes de un terminal a conectar de nuevo cuando el plano de reenvío determina que el paquete de protocolo de acceso es el paquete de inicio de autenticación; o

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en una cola de paquetes del terminal conectado cuando el plano de reenvío determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el plano de reenvío determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado; y

programar, por el plano de reenvío, la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado según las respectivas prioridades de la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado, en donde la prioridad de la cola de paquetes del terminal a conectar de nuevo es distinta de la prioridad de la cola de paquetes del terminal conectado.

3. El método de acuerdo con la reivindicación 2, en donde el elemento comprende adicionalmente un estado de autenticación del terminal conectado, el estado de autenticación se encuentra en autenticación incompleta o en autenticación completada, la cola de paquetes del terminal conectado comprende una cola de paquetes bajo autenticación y una cola de paquetes de autenticación completada, y una prioridad de la cola de paquetes bajo autenticación es distinta a una prioridad de la cola de paquetes de autenticación completada; y

el posicionamiento, por un plano de reenvío, el paquete de protocolo de acceso en una cola de paquetes del terminal conectado comprende:

determinar, por el plano de reenvío, un estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en la cola de paquetes bajo autenticación cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta; o

posicionar, por el plano de reenvío, el paquete de protocolo de acceso en la cola de paquetes de autenticación completada cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada.

4. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde el elemento comprende adicionalmente el estado de autenticación del terminal conectado, y el estado de autenticación se encuentra en autenticación incompleta o autenticación completada, y el método comprende adicionalmente:

cuando el plano de reenvío determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el plano de reenvío determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, determinar, por el plano de reenvío, el estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta y cuando el plano de reenvío determina que el paquete de protocolo de acceso es un paquete en línea; o

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete

de protocolo de acceso se encuentra en autenticación completada y cuando el plano de reenvío determina que el paquete de protocolo de acceso es un paquete de autenticación distinto al paquete de inicio de autenticación.

5. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde el método comprende adicionalmente:

recibir, por el plano de reenvío, una indicación que se envía por el plano de control, en donde la indicación se emplea para indicar que una cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a una cantidad preestablecida; y

limitar, por el plano de reenvío, una velocidad a la que se envía el paquete de inicio de autenticación al plano de control.

6. Un aparato de procesamiento de paquetes, en donde el aparato comprende:

una unidad de recepción, configurada para recibir un elemento que procede de un plano de control y recibir un paquete de protocolo de acceso, en donde el elemento comprende un identificador de un terminal conectado; y

una unidad de procesamiento, configurada para: cuando se determina que el paquete de protocolo de acceso no es un paquete de inicio de autenticación, determinar, según el identificador del terminal conectado, si un terminal servido por el paquete de protocolo de acceso es el terminal conectado, en donde el paquete de inicio de autenticación es un paquete de autenticación que se emplea para iniciar un proceso de autenticación para un terminal servido por el paquete de inicio de autenticación; y descartar, el paquete de protocolo de acceso cuando el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el terminal servido por el paquete de protocolo de acceso no es el terminal conectado.

7. El aparato de acuerdo con la reivindicación 6, en donde la unidad de procesamiento está configurada adicionalmente para:

posicionar el paquete de protocolo de acceso en una cola de paquetes de un terminal a conectar de nuevo cuando se determina que el paquete de protocolo de acceso es el paquete de inicio de autenticación; o

posicionar el paquete de protocolo de acceso en una cola de paquetes del terminal conectado cuando se determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y cuando se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado; y

programar la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado según las respectivas prioridades de la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado, en donde la prioridad de la cola de paquetes del terminal a conectar de nuevo es distinta de la prioridad de la cola de paquetes del terminal conectado.

8. El aparato de acuerdo con la reivindicación 7, en donde el elemento comprende adicionalmente un estado de autenticación del terminal conectado, el estado de autenticación se encuentra en autenticación incompleta o en autenticación completada, la cola de paquetes del terminal conectado comprende una cola de paquetes bajo autenticación y una cola de paquetes de autenticación completada, y una prioridad de la cola de paquetes bajo autenticación es distinta a una prioridad de la cola de paquetes de autenticación completada; y

la unidad de procesamiento está configurada para:

cuando se determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y cuando se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, determinar un estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

posicionar el paquete de protocolo de acceso en la cola de paquetes bajo autenticación cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta; o

posicionar el paquete de protocolo de acceso en la cola de paquetes de autenticación completada cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada.

9. El aparato de acuerdo con una cualquiera de las reivindicaciones 6 a 8, en donde el elemento comprende adicionalmente el estado de autenticación del terminal conectado, y el estado de autenticación se encuentra en autenticación incompleta o autenticación completada, y la unidad de procesamiento se configura adicionalmente para:

cuando se determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y cuando se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, determinar el estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta y cuando se determina que el paquete de protocolo de acceso es un paquete en línea; o

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada y cuando se determina que el paquete de protocolo de acceso es un paquete de autenticación distinto al paquete de inicio de autenticación.

10. El aparato de acuerdo con una cualquiera de las reivindicaciones 6 a 9, en donde

la unidad de recepción se configura adicionalmente para recibir una indicación que se envía por el plano de control, en donde la indicación se emplea para indicar que una cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a una cantidad preestablecida; y

la unidad de procesamiento se configura adicionalmente para limitar un velocidad a la que se envía el paquete de inicio de autenticación al plano de control.

11. Un dispositivo de procesamiento de paquetes, en donde el dispositivo comprende:

un aparato (10) de plano de control y un aparato (20) de plano de reenvío, en donde

el aparato (10) de plano de control está configurado para enviar un elemento al aparato de plano de reenvío, en donde el elemento comprende un identificador de un terminal conectado; y

el aparato (20) de plano de reenvío está configurado para recibir el elemento que procede del aparato (10) de plano de control y recibir un paquete de protocolo de acceso; cuando se determina que el paquete de protocolo de acceso no es un paquete de inicio de autenticación, determinar, según el identificador del terminal conectado, si un terminal servido por el paquete de protocolo de acceso es el terminal conectado, en donde el paquete de inicio de autenticación es un paquete de autenticación que se emplea para iniciar un proceso de autenticación para un terminal servido por el paquete de inicio de autenticación; y descartar, el paquete de protocolo de acceso cuando el paquete de protocolo de acceso no es el paquete de inicio de autenticación y el terminal servido por el paquete de protocolo de acceso no es el terminal conectado.

12. El dispositivo de acuerdo con la reivindicación 11, en donde el aparato (20) de plano de reenvío está configurado adicionalmente para:

posicionar el paquete de protocolo de acceso en una cola de paquetes de un terminal a conectar de nuevo cuando se determina que el paquete de protocolo de acceso es el paquete de inicio de autenticación; o

posicionar el paquete de protocolo de acceso en una cola de paquetes del terminal conectado cuando se determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y cuando se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado; y

programar la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado según las respectivas prioridades de la cola de paquetes del terminal a conectar de nuevo y la cola de paquetes del terminal conectado, en donde la prioridad de la cola de paquetes del terminal a conectar de nuevo es distinta de la prioridad de la cola de paquetes del terminal conectado.

13. El dispositivo de acuerdo con la reivindicación 12, en donde el elemento comprende adicionalmente un estado de autenticación del terminal conectado, el estado de autenticación se encuentra en autenticación incompleta o en autenticación completada, la cola de paquetes del terminal conectado comprende una cola de paquetes bajo autenticación y una cola de paquetes de autenticación completada, y una prioridad de la cola de paquetes bajo autenticación es distinta a una prioridad de la cola de paquetes de autenticación completada; y

el aparato (20) de plano de reenvío se configura adicionalmente para:

cuando se determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y cuando se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, determinar un estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

posicionar el paquete de protocolo de acceso en la cola de paquetes bajo autenticación cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta; o

posicionar el paquete de protocolo de acceso en la cola de paquetes de autenticación completada cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada.

14. El dispositivo de acuerdo con una cualquiera de las reivindicaciones 11 a 13, en donde el elemento comprende

adicionalmente el estado de autenticación del terminal conectado, y el estado de autenticación se encuentra en autenticación incompleta o autenticación completada, y el aparato (20) de plano de reenvío se configura adicionalmente para:

cuando se determina que el paquete de protocolo de acceso no es el paquete de inicio de autenticación y cuando se determina que el terminal servido por el paquete de protocolo de acceso es el terminal conectado, determinar el estado de autenticación del terminal servido por el paquete de protocolo de acceso; y

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación incompleta y cuando se determina que el paquete de protocolo de acceso es un paquete en línea; o

descartar el paquete de protocolo de acceso cuando el estado de autenticación del terminal servido por el paquete de protocolo de acceso se encuentra en autenticación completada y cuando se determina que el paquete de protocolo de acceso es un paquete de autenticación distinto al paquete de inicio de autenticación.

15. El dispositivo de acuerdo con una cualquiera de las reivindicaciones 11 a 14, en donde

el aparato (10) de plano de control se configura adicionalmente para enviar una indicación al aparato (20) de plano de reenvío, en donde la indicación se emplea para indicar que una cantidad de terminales conectados cuyo estado de autenticación se encuentra en autenticación incompleta es superior a una cantidad preestablecida; y

el aparato (20) de plano de reenvío se configura adicionalmente para recibir la indicación que se envía por el aparato (10) de plano de control, y limitar una velocidad a la que se envía el paquete de inicio de autenticación al aparato (10) de plano de control.

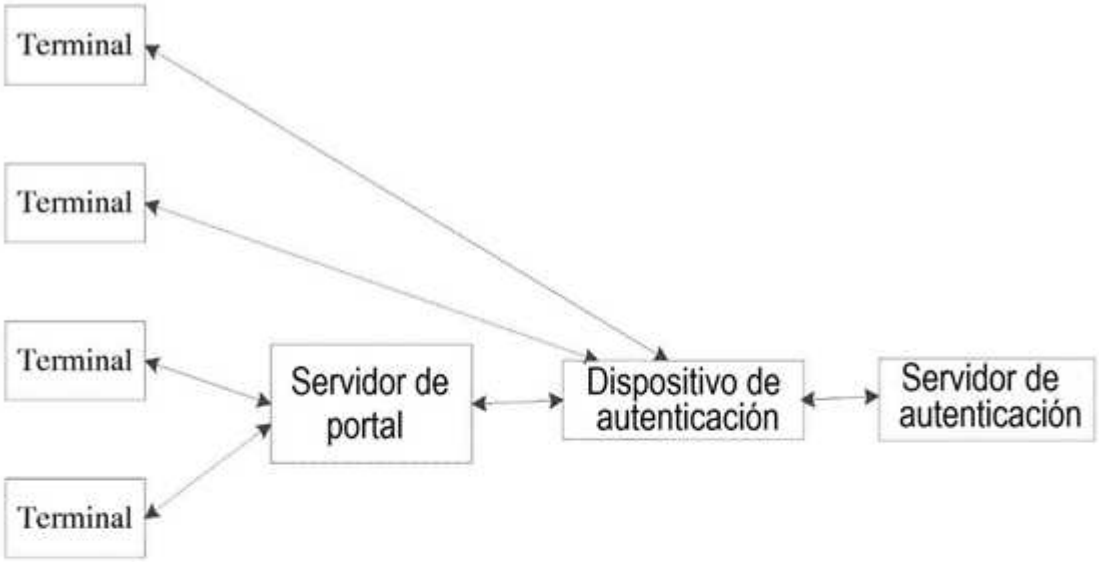
Terminal
Terminal
Terminal
Terminal
Servidor de portal
Dispositivo de autenticación
Servidor de autenticación

FIG. 1

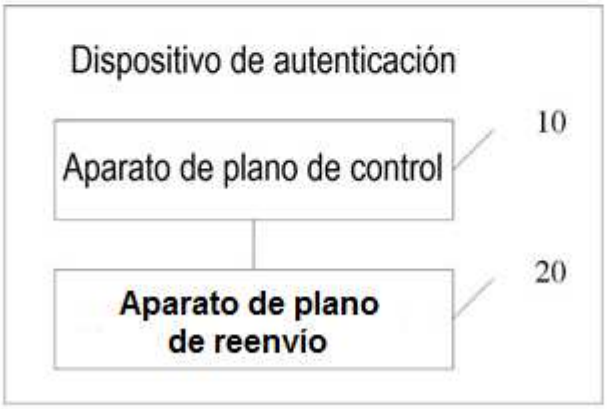
Dispositivo de autenticación
Aparato de plano de control
10
Aparato de plano de reenvío
20

FIG. 2

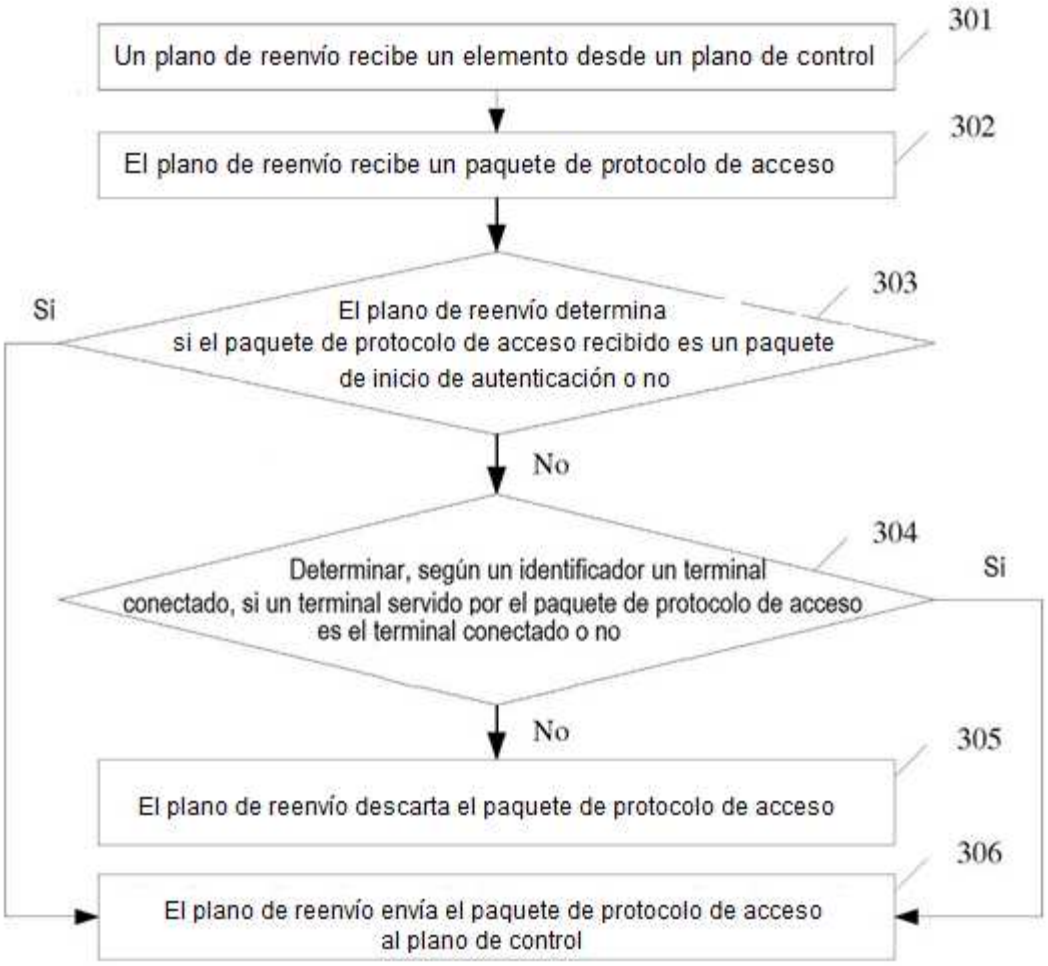

FIG. 3

Formato de un paquete EAPOL

Tipo de Ethernet de entidad de acceso de puerto	
Versión de protocolo	Tipo
Longitud	
Cuerpo de paquete	

FIG. 4