(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 634 690**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.07.2014 PCT/CN2014/081326**

(87) Fecha y número de publicación internacional: **15.01.2015 WO15003565**

(96) Fecha de presentación y número de la solicitud europea: **01.07.2014 E 14822073 (4)**

(97) Fecha y número de publicación de la concesión europea: **07.06.2017 EP 3001635**

(54) Título: **Método, dispositivo y sistema para controlar el acceso a un terminal de usuario**

(30) Prioridad:

09.07.2013 CN 201310286753

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.09.2017

(73) Titular/es:

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

(72) Inventor/es:

SUN, BING;
XU, YIBIN y
TANG, PENGHE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, dispositivo y sistema para controlar el acceso a un terminal de usuario

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de tecnologías de comunicaciones y en particular, a un método, un aparato y un sistema para controlar el acceso de un terminal de usuario.

ANTECEDENTES DE LA INVENCIÓN

En un sistema de comunicaciones, una red de campo (en inglés: campus network, CAN en forma abreviada) se refiere, en general a una red de un campus o una intrared (en inglés: intranet) de una empresa, y una característica principal de la red de campus es que un enrutador, un conmutador de red y un dispositivo similar dispuesto en la red de campus se gestiona por una organización de gestión (a modo de ejemplo, un propietario de la red de campus).

Según se ilustra en la Figura 1, en una arquitectura de red de una red de campus, la red de campus incluye al menos un terminal de usuario y al menos un conmutador de red. En general, un conmutador de red que está situado en un lado del terminal de usuario y está directamente conectado a un terminal de usuario puede denominarse como un conmutador de acceso a un nodo de conmutación de acceso. En términos generales, un conmutador de red que está situado en un lado de la red y está conectado a un nodo de conmutación de acceso puede denominarse un conmutador de agregación o un nodo de conmutación de agregación. Cada interfaz en cada nodo de conmutación de acceso puede no estar conectada a cualquier terminal de usuario, o puede conectarse a al menos un terminal de usuario. Si un terminal de usuario está conectado a un nodo de conmutación de acceso, el terminal de usuario puede estar conectado al nodo de conmutación de acceso en una manera cableada. Una interfaz en el otro lado del nodo de conmutación de acceso está conectada a un nodo de conmutación de agregación, para realizar una transmisión de paquetes. En la arquitectura de red de la red de campus ilustrada en la Figura 1, después de que un terminal de usuario esté satisfactoriamente conectado a un nodo de conmutación de acceso en una manera cableada, necesita realizarse una autenticación antes de la transmisión del paquete para comprobar si al terminal de usuario le está permitido acceder a la red de campus para transmisión de paquetes. El terminal de usuario puede enviar un paquete al nodo de conmutación de acceso solamente cuando al terminal de usuario le esté permitido acceder a la red de campus para la transmisión de paquetes. En términos generales, existen dos maneras de realizar la autenticación para comprobar si a un terminal de usuario le está permitido acceder a una red de campus para la transmisión de paquetes, para controlar si el terminal de usuario puede acceder, o no, a la red de campus para la transmisión de paquetes.

Una primera manera consiste en: un nodo de conmutación de acceso realiza la autenticación comprobar si a un terminal de usuario le está permitido acceder a una red de campus para la transmisión de paquetes, es decir, el nodo de conmutación de acceso realiza una autenticación sobre el acceso del terminal de usuario, y determina, en conformidad con un resultado de resultado, si al terminal de usuario le está permitido, o no, acceder a la red de campus para la transmisión de paquetes. La arquitectura de red de la red de campus ilustrada en la Figura 1, se utiliza, a modo de ejemplo, en donde un terminal de usuario 1 y un terminal de usuario 2 están conectados a un nodo de conmutación de acceso 1 en una manera cableada, un terminal de usuario 3 está conectado a un nodo de conmutación de acceso 2 en una manera cableada, y ambos, el nodo de conmutación de acceso 1 y el nodo de conmutación de acceso 2 están conectados a un nodo de conmutación de agregación. En una puesta en práctica específica, el nodo de conmutación de acceso 1 realiza la autenticación para comprobar si al terminal de usuario 1 y al terminal de usuario 2 les está permitido acceder a la red de campus, y el nodo de conmutación de acceso 2 realiza la autenticación para comprobar si al terminal de usuario 3 le está permitido acceder a la red de campus. El terminal de usuario 1, el terminal de usuario 2 o el terminal de usuario 3 pueden acceder a la red para transmisión de paquetes solamente en un caso en el que sea satisfactoria la autenticación. En un caso en el que se utilice la primera manera, cada nodo de conmutación de acceso en un sistema necesita poner en práctica una autenticación de acceso sobre un terminal de usuario conectado al nodo de conmutación de acceso. Sin embargo, en general, puesto que existen numerosos nodos de comunicación de acceso en el sistema, la complejidad de la arquitectura de red utilizada en la primera manera es relativamente alta.

Una segunda manera consiste en: un nodo de conmutación de agregación realiza una autenticación sobre el acceso de un terminal de usuario. En la arquitectura del sistema ilustrada en la Figura 1, el nodo de conmutación de agregación realiza la autenticación sobre cualquier terminal de usuario en el sistema que está conectado a un nodo de conmutación de acceso. Si la autenticación es satisfactoria, el nodo de conmutación de agregación permite a todos los terminales de usuario que estén conectados al nodo de conmutación de acceso, acceder a la red. Es decir, en esta manera, después de que se realice la autenticación de acceso por el nodo de conmutación de agregación sobre cualquier terminal de usuario conectado al nodo de conmutación de acceso de forma satisfactoria, otro terminal de usuario conectado al nodo de conmutación de acceso no requiere la autenticación del acceso pero está directamente conectado a la red para la transmisión de paquetes utilizando el nodo de conmutación de acceso. En un caso en el que se utiliza la segunda manera, el control sobre un terminal de usuario único no se puede realizar y la seguridad es deficiente.

En conclusión, una manera de puesta en práctica de un método común para controlar el acceso de un terminal de usuario es relativamente completa o la seguridad es relativamente deficiente.

El documento CN 101 980 496 A da a conocer un método de autenticación que implica la información del puerto de acceso. La información del puerto de acceso se utiliza para generar información de aprendizaje de MAC.

El documento de Cheswick et. al: “Firewalls y seguridad de Internet – 2ª edición” en: “USA”, 1 de enero de 2003, Addison Wesley, XP055253011, da a conocer túneles de red VPN entre dispositivos.

SUMARIO DE LA INVENCIÓN

La presente invención da a conocer un método, un aparato y un sistema para controlar el acceso de un terminal de usuario, que puede mejorar la seguridad de la red en un caso en el que un procedimiento de puesta en práctica de la autenticación del acceso realizado en un terminal de usuario está simplificado.

De conformidad con un primer aspecto de la idea inventiva, se da a conocer un método para controlar el acceso de un terminal de usuario, en donde el método incluye: recibir, por un controlador, un paquete de autenticación enviado por un nodo de conmutación de acceso por intermedio de un túnel de datos establecido; obtener, por el controlador, una dirección MAC en un campo de dirección MAC origen del paquete de autenticación; después de una autenticación del acceso se realice en un terminal de usuario correspondiente a la dirección MAC obtenida de forma satisfactoria, determinar, a partir de una correspondencia mantenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, en donde el identificador de interfaz es un identificador de interfaz de una interfaz en el nodo de conmutación de acceso conectado al terminal de usuario; y enviar, por el controlador, el identificador de interfaz determinado al nodo de conmutación de acceso por intermedio de un túnel de control establecido entre el lado y el nodo de conmutación de acceso, y dar instrucciones al nodo de conmutación de acceso para activar la interfaz correspondiente al identificador de interfaz.

En una primera manera de puesta en práctica posible del primer aspecto de la idea inventiva, antes de se realice la autenticación de acceso en el terminal de usuario correspondiente a la dirección MAC, se determina la correspondencia entre una dirección MAC de un terminal de usuario y un identificador de interfaz en la manera siguiente: recibir, por el controlador, la dirección MAC del terminal de usuario enviada por el nodo de conmutación de acceso por intermedio del túnel de control, y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario se obtiene por el nodo de conmutación de acceso cuando el terminal de usuario establece una conexión con la interfaz en el nodo de conmutación de acceso, y envía un paquete por intermedio de la interfaz conectada; y establecer una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido.

En conformidad con un segundo aspecto de la idea inventiva, se da a conocer un método para controlar el acceso de un terminal de usuario, en donde el método incluye: cuando se desactiva una función de aprendizaje de control de acceso al soporte MAC, recibir, por un nodo de conmutación de acceso, un paquete de autenticación enviado por un terminal de usuario que está conectado a una interfaz en el nodo de conmutación de acceso; obtener, por el nodo de conmutación de acceso, un identificador de interfaz de la interfaz conectada al terminal de usuario y envía el paquete de autenticación, y obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido; enviar, por el nodo de conmutación de acceso, la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido a un controlador por intermedio de un túnel de control establecido, de modo que el controlador mantenga una correspondencia entre la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido; recibir, por el nodo de conmutación de acceso, el identificador de interfaz enviado por el controlador por intermedio del túnel de control, en donde el identificador de interfaz es un identificador de interfaz que se determina a partir de la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz después de que el controlador realice satisfactoriamente una autenticación de acceso en el terminal de usuario correspondiente a la dirección MAC, y está en correspondencia con la dirección MAC del terminal de usuario satisfactoriamente autenticado; y activar, por el nodo de conmutación de acceso en conformidad con el identificador de interfaz recibido, la interfaz correspondiente a dicha interfaz.

En una primera posible manera de puesta en práctica del segundo aspecto de la idea inventiva, el método incluye, además: recibir, por el nodo de conmutación de acceso, un permiso de acceso que es del terminal de usuario correspondiente a la dirección MAC y se envía por el controlador por intermedio del túnel de control; y la activación, por el nodo de conmutación de acceso en conformidad con el identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz incluye: configurar o modificar, en conformidad con un permiso de acceso recibido enviado por un nodo de conmutación de agregación, el permiso de acceso de la interfaz que está en un nodo de conmutación de acceso y corresponde al identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para acceder a un red de conformidad con el permiso de acceso.

Con referencia al segundo aspecto de la idea inventiva o la primera manera de puesta en práctica posible del segundo aspecto, en una segunda manera de puesta en práctica posible del segundo aspecto, la obtención, por el nodo de conmutación de acceso, de un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido incluye: determinar, por el nodo de conmutación de acceso utilizando un procesador de señal que es capaz de realizar una función de procesamiento en conformidad con un código de programa, el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y transmitir el paquete de autenticación recibido al procesador de señal del nodo de conmutación de acceso; y obtener, por el procesador de señal, a partir de un campo de dirección MAC origen del paquete de autenticación, la dirección MAC del terminal de usuario que envía el paquete de autenticación.

En conformidad con un tercer aspecto de la idea inventiva, se da a conocer un aparato para controlar el acceso de un terminal de usuario, en donde el aparato incluye: un módulo de recepción, configurado para: recibir un paquete de autenticación enviado por intermedio de un túnel de datos establecido, y transmitir el paquete de autenticación recibido a un módulo de obtención; el módulo de obtención, configurado para: obtener el paquete de autenticación transmitido por el módulo de recepción, obtener una dirección MAC en un campo de dirección de MAC origen del paquete de autenticación y transmitir la dirección MAC obtenida a un módulo de autenticación; el módulo de autenticación, configurado para: recibir la dirección MAC transmitida por el módulo de obtención, realizar la autenticación de acceso sobre un terminal de usuario correspondiente a la dirección MAC, y transmitir un resultado de la autenticación satisfactoria a un módulo de determinación; el módulo de determinación, configurado para: obtener el resultado de autenticación satisfactoria transmitido por el módulo de autenticación; determinar, a partir de una correspondencia mantenida entre la dirección MAC de un terminal de usuario y un identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, en donde el identificador de interfaz es un identificador de interfaz de una interfaz en un nodo de conmutación de acceso conectado al terminal de usuario; y transmitir el identificador de interfaz a un módulo de envío; y el módulo de envío, configurado para: obtener el identificador de interfaz transmitido por el módulo de determinación, enviar el identificador de interfaz determinado a un nodo de conmutación de acceso por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, y dar instrucciones al nodo de conmutación de acceso para activar la interfaz correspondiente a al identificador de interfaz.

En una primera manera de puesta en práctica posible del tercer aspecto de la idea inventiva, el módulo de recepción está configurado, además, para: recibir la dirección MAC del terminal de usuario enviada por el nodo de conmutación de acceso por intermedio del túnel de control, y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectada al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario se obtienen por el nodo de conmutación de acceso cuando el terminal de usuario establece una conexión con la interfaz en el nodo de conmutación de acceso, y enviar un paquete por intermedio de la interfaz conectada; y transmitir la dirección MAC recibida y el identificador de interfaz recibido a un módulo de establecimiento; y el aparato comprende, además, el módulo de establecimiento, configurado para: obtener la dirección MAC y el identificador de interfaz que se transmiten por el módulo de recepción, y establecer una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido.

En conformidad con un cuarto aspecto de la idea inventiva, se da a conocer un aparato de controlar el acceso de un terminal de usuario, en donde el aparato incluye: un módulo de recepción, configurado para: cuando se desactiva una función de aprendizaje de control de acceso al soporte MAC, recibir un paquete de autenticación enviado por un terminal de usuario que está conectado a una interfaz en el nodo de conmutación de acceso, y transmitir el paquete de autenticación a un módulo de obtención; el módulo de obtención, configurado para: recibir el paquete de autenticación transmitido por el módulo de recepción, obtener un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido y transmitir el identificador de interfaz y la dirección MAC a un módulo de envío; el módulo de envío, configurado para: recibir el identificador de interfaz y la dirección MAC que se transmiten por el módulo de obtención, y enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido a un controlador por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, de modo que el controlador mantenga una correspondencia entre la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido, en donde el módulo recepción está configurado, además, para: recibir el identificador de interfaz enviado por el controlador por intermedio del túnel de control, y transmitir el identificador de interfaz a un módulo de control, en donde el identificador de interfaz es un identificador de interfaz que se determina a partir de la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz después de que el controlador realice de forma satisfactoria la autenticación de acceso del terminal de usuario correspondiente a la dirección MAC, y está en correspondencia con la dirección MAC del terminal de usuario satisfactoriamente autenticado; y el módulo de control, configurado para: obtener el identificador de interfaz transmitido por el módulo de recepción y activar, en función del identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz.

En una primera manera de puesta en práctica posible del cuarto aspecto de la idea inventiva, el módulo de recepción está configurado, además, para: recibir un permiso de acceso que es del terminal de usuario correspondiente a la dirección MAC y se envía por el controlador por intermedio del túnel de control, y transmitir el permiso de control al módulo de control; y el módulo de control está configurado específicamente para: obtener el permiso de acceso transmitido por el módulo de recepción y configurar o modificar, en conformidad con un permiso de acceso recibido enviado por un nodo de conmutación de agregación, el permiso de acceso de la interfaz que está en el nodo de conmutación de acceso y correspondiente al identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para acceder a una red de conformidad con el permiso de acceso.

Con referencia al cuarto aspecto o la primera manera de puesta en práctica posible del cuarto aspecto de la idea inventiva, en una segunda manera de puesta en práctica posible del cuarto aspecto, el módulo de obtención incluye específicamente un procesador de señal, y está configurado para: determinar el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y obtener el paquete de autenticación transmitido por el módulo de recepción; y el procesador de señal obtiene, a partir de un campo de dirección MAC origen del paquete de autenticación, la dirección MAC del terminal de usuario que envía el paquete de autenticación.

En las soluciones técnicas dadas a conocer en la presente invención, después de la realización satisfactoria de la autenticación de acceso en un terminal de usuario, un identificador de interfaz correspondiente a una dirección MAC del terminal de usuario satisfactoriamente autenticado se determina a partir de una correspondencia obtenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, el identificador de interfaz determinado se envía a un nodo de conmutación de acceso por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, y el nodo de conmutación de acceso da instrucciones para activar una interfaz correspondiente al identificador de interfaz. De este modo, las redes de acceso y los permisos de acceso de redes de terminales de usuario pueden controlarse de una manera centralizada, una arquitectura del sistema es relativamente simple y es fácil de ponerse en práctica, y la seguridad de la red puede mejorarse todavía más.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama esquemático de una arquitectura de red de un sistema parar controlar el acceso de un terminal de usuario;

La Figura 2 es un diagrama estructural esquemático de composición de un primer sistema para controlar el acceso de un terminal de usuario en conformidad con la forma de realización 1 de la presente invención;

La Figura 3a es un diagrama esquemático que ilustra una aplicación del protocolo CAPWAP en una arquitectura de sistema WLAN;

La Figura 3b es un diagrama estructural esquemático de un paquete de datos CAPWAP transmitido por intermedio de un túnel de datos;

La Figura 3c es un diagrama estructural esquemático de composición de una cabecera de un paquete de datos CAPWAP transmitido por intermedio de un túnel de datos;

La Figura 3d es un diagrama estructural esquemático de un paquete de control CAPWAP transmitido por intermedio de un túnel de control;

La Figura 3e es un diagrama estructural esquemático de composición de una cabecera de un paquete de control CAPWAP transmitido por intermedio de un túnel de control;

La Figura 4 es un diagrama estructural esquemático de composición de un segundo sistema para controlar el acceso de un terminal de usuario en conformidad con la forma de realización 1 de la presente invención;

La Figura 5 es un diagrama de flujo de un método para controlar el acceso de un terminal de usuario en conformidad con la forma de realización 2 de la presente invención;

La Figura 6a es un diagrama de flujo de un método para controlar el acceso de un terminal de usuario en conformidad con la forma de realización 3 de la presente invención, en donde el método se aplica a un lado del nodo de conmutación de agregación;

La Figura 6b es un diagrama estructural esquemático de composición de un aparato para controlar el acceso de un terminal de usuario en conformidad con la forma de realización 3 de la presente invención;

La Figura 6c es un diagrama estructural esquemático de un conmutador de red en conformidad con la forma de realización 3 de la presente invención;

La Figura 7a es un diagrama de flujo de un método para controlar el acceso de un terminal de usuario en conformidad con la forma de realización 3 de la presente invención, en donde el método se aplica a un lado del nodo de conmutación de acceso;

La Figura 7b es un diagrama estructural esquemático de composición de un aparato para controlar el acceso de un terminal de usuario en conformidad con la forma de realización 3 de la presente invención; y

La Figura 7c es un diagrama estructural esquemático de composición de un conmutador de red en conformidad con la forma de realización 3 de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

Para un problema común de que una manera de puesta en práctica de un método para controlar el acceso de un terminal de usuario es relativamente complejo o la seguridad es relativamente deficiente, se proporcionan soluciones técnicas en formas de realización de la presente invención. En las soluciones técnicas, después de realizada una autenticación de acceso en un terminal de usuario de forma satisfactoria, un identificador de interfaz correspondiente a una dirección MAC del terminal de usuario satisfactoriamente autenticado se determina a partir de una correspondencia obtenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, el identificador de interfaz determinado se envía a un nodo de conmutación de acceso por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, y el nodo de conmutación de acceso recibe instrucciones para activar una interfaz correspondiente al identificador de interfaz. De este modo, las redes de acceso y los permisos de acceso de red de terminales de usuario pueden controlarse de una manera centralizada, una arquitectura de sistema es relativamente simple y fácil de poner en práctica, y se puede mejorar todavía más la seguridad de la red.

Con referencia a los dibujos adjuntos, a continuación se describe, en detalle, los principios de puesta en práctica claves, las maneras de puesta en práctica específicas y las ventajas de las soluciones técnicas en la presente invención.

Las soluciones técnicas dadas a conocer en las formas de realización de la presente invención pueden ponerse en práctica utilizando un controlador. El controlador puede disponerse en una red como un dispositivo de red independiente, o puede integrarse, como un módulo integrado, en un nodo de conmutación de agregación dispuesto en una red, y sus detalles se describen a continuación respectivamente.

Forma de realización 1

La forma de realización 1 de la presente invención da a conocer un sistema para controlar el acceso de un terminal de usuario. Un controlador está integrado en un nodo de conmutación de agregación como un módulo de integrado, para poner en práctica las soluciones técnicas dadas a conocer en la forma de realización 1 de la presente invención. Según se ilustra en la Figura 2, el sistema incluye al menos un nodo de conmutación de acceso y al menos un nodo de conmutación de agregación, en donde cada nodo de conmutación de acceso del al menos un nodo de conmutación de acceso está conectado a un nodo de conmutación de agregación del al menos un nodo de conmutación de agregación. Cualquier nodo de conmutación de acceso del al menos un nodo de conmutación de acceso puede conectarse a al menos un terminal de usuario en una manera cableada, o puede no conectarse a cualquier terminal de usuario, es decir, una interfaz utilizada para conectar a un terminal de usuario está en un estado inactivo.

Un túnel de transmisión de paquetes se establece entre un nodo de conmutación de agregación y un nodo de conmutación de acceso. El túnel de transmisión de paquetes entre el nodo de conmutación de agregación y el nodo de conmutación de acceso puede establecerse de conformidad con un protocolo propietario prestablecido o extendiendo un protocolo estándar. A modo de ejemplo, el protocolo estándar puede ser el protocolo de Control y Aprovisionamiento de Puntos de Acceso Inalámbricos (en inglés: Control And Provisioning of Wireless Access Points, CAPWAP en forma abreviada). En esta forma de realización de la presente invención, en la que un túnel de transmisión de paquetes se establece extendiendo el protocolo CAPWAP tal como se utiliza como un ejemplo para la descripción detallada. El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP extendido incluye un túnel de control para transmitir un paquete de control y un túnel de datos para transmitir un paquete de datos.

El protocolo CAPWAP es un protocolo estándar aplicado a un entorno de comunicaciones inalámbricas. En el entorno de comunicaciones inalámbricas, el protocolo CAPWAP se aplica a un escenario operativo de interfuncionamiento entre un nodo de acceso de control (en inglés: access control, AC en forma abreviada) y un punto de acceso inalámbrico (en inglés: access point, AP en forma abreviada). Según se ilustra en la Figura 3a, el entorno de comunicaciones inalámbricas sobre la base del protocolo CAPWAP incluye un punto de acceso AP inalámbrico, un conmutador de red, un control de acceso AC y un terminal de usuario. El punto de acceso AP inalámbrico está conectado a al menos un terminal de usuario en una manera inalámbrica. El túnel de transmisión de paquetes para transmitir un paquete en una manera inalámbrica se establece entre el punto de acceso AP

inalámbrico y el AC sobre la base del protocolo CAPWAP. El túnel de control establecido entre el punto de acceso AP inalámbrico y el control AC utilizando el protocolo CAPWAP se utiliza para intercambiar un paquete de control entre el AC y el AP inalámbrico; y el túnel de datos establecido el AP inalámbrico y el AC utilizando el protocolo CAPWAP se utiliza para transmitir un paquete de datos enviado por un terminal de usuario. El paquete de datos transmitido por intermedio del túnel de datos y el paquete de control transmitido por intermedio del túnel de control, pueden transmitirse en una manera no encriptada. El protocolo de Seguridad de Capa de Transporte de Datagrama (en inglés: Datagram Transport Layer Security, DTLS) puede utilizarse también para encriptación, para mejorar la seguridad del paquete de datos transmitido por intermedio del túnel de datos y la del paquete de control transmitido por el intermedio del túnel de control. En la forma de realización 1 de la presente invención, en donde el protocolo DTLS se utiliza para encriptar el paquete de datos transmitido por intermedio del túnel de datos y el paquete de control transmitido por el intermedio del túnel de control se utiliza a modo de ejemplo, para describir, todavía más, la composición estructural del paquete de datos y la del paquete de control.

El diagrama estructural esquemático de composición del paquete de datos transmitido por intermedio del túnel de datos establecido utilizando el protocolo CAPWAP se ilustra en la Figura 3b. En la composición estructural del paquete de datos transmitidos por intermedio del túnel de datos, el paquete de datos incluye una cabecera de dirección IP (IP Hdr en forma abreviada en el diagrama), una cabecera de Protocolo de Datagrama del Usuario (en inglés: User Datagram Protocol, UDP en forma abreviada), (UDP Hdr ilustrada en el diagrama), una cabecera DTLS (DTLS Hdr ilustrada en el diagrama), una cabecera de paquete CAPWAP (CAPWAP Hdr ilustrada en el diagrama) y una carga útil inalámbrica (en inglés: Wireless payload), en donde la carga útil inalámbrica se utiliza para transmitir datos. Más concretamente, en la composición estructural de la cabecera CAPWAP Hdr ilustrada en la Figura 3c, la cabecera CAPWAP Hdr incluye un identificador de campo, un desplazamiento de campo, un campo de dirección MAC inalámbrico opcional u otra información inalámbrica opcional.

La Figura 3d es un diagrama estructural esquemático de composición de un paquete de control CAPWAP transmitido por intermedio del túnel de control. En una estructura del paquete de control CAPWAP transmitido por intermedio del túnel de control, el paquete de control CAPWAP incluye una cabecera de dirección IP (IP Hdr ilustrada en el diagrama), una cabecera UDP (UDP Hdr ilustrada en el diagrama), una cabecera DTLS (DTLS Hdr ilustrada en el diagrama), una cabecera de paquete CAPWAP (CAPWAP Hdr ilustrada en el diagrama), un campo de cabecera de control (en inglés: Control Header) que se utiliza para transmitir una función del paquete de control y un campo de elemento de mensaje (en inglés: Message Element) utilizado para transmitir el contenido del paquete de control. El contenido del paquete de control puede denominarse como información de control. La composición estructural de una cabecera de control del paquete de control CAPWAP se ilustra en la Figura 3e. La información de control transmitida en el campo de elemento de mensaje puede ser valores de longitud tipo (en inglés: type-length-value, TLV en forma abreviada) de diferentes tipos, en donde T es un tipo de la información de control, L es una longitud de la información de control y V es un valor de la información de control. En una puesta en práctica real, el valor de la información de control en el TLV puede extenderse, es decir, en un TLV, pueden incluirse, además, múltiples TLVs extendidos incluidos en el valor V de la información de control, y estos TLVs extendidos pueden denominarse TLVs de nivel 2. Más concretamente, en el campo de elemento de mensaje, si un valor de T en el TLV es 37, el TLV se utiliza para realizar una extensión del contenido en la información de control. En las soluciones técnicas dadas a conocer en la forma de realización 1 de la presente invención, una manera de añadir un TLV de nivel 2 al elemento de mensaje en el que el valor de T es 37 se utiliza para realizar una extensión del contenido en el mensaje de control. Más concretamente, el elemento de mensaje en el que el valor de T es 37 puede denominarse como elemento de mensaje nº 37, en donde un formato estándar del elemento de mensaje nº 37 se ilustra en la tabla 1.

Tabla 1

Tipo de elemento de mensaje: 37, información definida por un proveedor de dispositivos, 2 bytes
Longitud del elemento de mensaje: 2 bytes
Identificador del proveedor: valores que no son los mismos para diferentes fabricantes de dispositivos, 4 bytes
ID de elemento: 2 bytes
Datos

En la tabla 1, los valores del campo de identificador del proveedor no son los mismos para diferentes fabricantes de dispositivos. A modo de ejemplo, un valor 2011 se utiliza como un ejemplo para la descripción detallada en las soluciones técnicas dadas a conocer en esta forma de realización de la presente invención y el ejemplo se utiliza también en la descripción siguiente.

El formato estándar del elemento de mensaje nº 37 se extiende, y un formato extendido del elemento de mensaje se ilustra en la tabla 2.

Tabla 2

Tipo de elemento de mensaje: 37, información definida por un proveedor de dispositivos, 2 bytes
Longitud del elemento de mensaje: 2 bytes
Identificador del proveedor: un valor de 2011, 4 bytes
Tipo 1 de TLV nivel 2: 2 bytes
Longitud 1 del TLV de nivel 2: 2 bytes
Contenido 1 del TLV de nivel 2: ampliado
Tipo 2 del TLV de nivel 2: 2 bytes
Longitud 2 del TLV de nivel 2: 2 bytes
Contenido 2 del TLV de nivel 2: ampliado
…..

El hecho de que el protocolo CAPWAP estándar se extienda para establecer un túnel de transmisión de paquetes entre un nodo de conmutación de acceso y un nodo de conmutación de agregación se utiliza, a modo de ejemplo, para describir en detalle las soluciones técnicas dadas a conocer en esta forma de realización de la presente invención. El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP extendido incluye un túnel de control para transmitir información de control y un túnel de datos para transmitir información de datos. En una arquitectura de sistema ilustrada en la Figura 2, se establece el túnel de transmisión entre el nodo de conmutación de agregación y el nodo de conmutación de acceso sobre la base del protocolo CAPWAP extendido. El hecho de que el nodo de conmutación de acceso esté conectado a al menos un terminal de usuario se utiliza, a modo de ejemplo, para la descripción detallada. El nodo de conmutación de acceso controla el reenvío de datos de todas las interfaces.

Después de que un terminal de usuario se conecte a una interfaz en el nodo de conmutación de acceso, el nodo de conmutación de acceso obtiene un identificador de interfaz de la interfaz conectada al terminal de usuario, obtiene una dirección de control de acceso al soporte (en inglés: media access control, MAC en forma abreviada) del terminal de usuario a partir del paquete recibido enviado por el terminal de usuario y envía la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de transmisión de paquetes establecido. El identificador de interfaz de la interfaz en el nodo de conmutación de acceso puede preestablecerse, o puede ser una forma de combinación de una identidad de dispositivo del nodo de conmutación de acceso y un número de secuencia (en inglés: sequence number) de la interfaz. A modo de ejemplo, si la identidad de dispositivo del nodo de conmutación de acceso es ID, y el nodo de conmutación de acceso incluye totalmente ocho interfaces numeradas de 1 a 8, los identificadores de interfaz de las ocho interfaces en el nodo de conmutación de acceso pueden representarse como ID1, ID2, … e ID8. El nodo de conmutación de acceso puede recibir un paquete enviado por el terminal de usuario conectado a la vez en el nodo de conmutación de acceso; determina, utilizando un procesador de señal del nodo de conmutación de acceso, el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete; extrae un campo de dirección MAC origen del paquete recibido utilizando el procesador de señal del nodo de conmutación de acceso, para obtener la dirección MAC del terminal de usuario; y enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de control que está incluido en el túnel de transmisión de paquetes establecido.

El procesador de señal del nodo de conmutación de acceso puede ser una unidad central de procesamiento (en inglés: central processing unit, CPU en forma abreviada), una combinación de una unidad CPU y un circuito integrado de hardware, un procesador de red (en inglés: network processor, NP en forma abreviada), una combinación de una unidad CPU y un procesador NP o una combinación de un procesador NP y un circuito integrado de hardware. El nodo de conmutación de agregación recibe la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz se envían por el nodo de conmutación de acceso por intermedio del túnel de transmisión de paquetes; y mantiene una correspondencia entre la dirección MAC del terminal de usuario en función de la dirección MAC recibida y el identificador de interfaz recibido. La correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz que se mantiene por el nodo de conmutación de agregación puede memorizarse en una manera de memorización intermedia. La correspondencia se memoriza dentro de un período de tiempo; después de completarse la autenticación de acceso realizada en el terminal de usuario, puede suprimirse la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz.

El nodo de conmutación de acceso tiene una función de aprendizaje de MAC (en inglés: MAC learning). La función de aprendizaje de MAC permite a un conmutador de red tener conocimiento de la dirección MAC de otro dispositivo

en una red, para identificar una interfaz a partir de la cual se envía un paquete cuya dirección de destino sea la dirección MAC. Sin embargo, cuando el nodo de conmutación de agregación realiza el control sobre el acceso del terminal de usuario, si la función de aprendizaje de MAC del nodo de conmutación de acceso no está desactiva, el terminal de usuario puede acceder, sin ser autenticado, a una red utilizando el nodo de conmutación de acceso. En este caso, no se puede controlar el acceso del terminal de usuario. En consecuencia, en un escenario operativo en el que el nodo de conmutación de agregación controla el acceso del terminal de usuario, la función de aprendizaje de MAC del nodo de conmutación de acceso está desactivada. En un caso en el que se desactiva la función de aprendizaje de MAC, el terminal de usuario no puede acceder directamente a una red y el nodo de conmutación de acceso no puede encontrar, en función de la dirección MAC del terminal de usuario, el identificador de interfaz de la interfaz conectada al terminal de usuario. Por lo tanto, en esta forma de realización de la presente invención, la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz se mantiene por el nodo de conmutación de agregación. Durante un proceso de puesta en práctica del control sobre el acceso del terminal de usuario, aunque el nodo de conmutación de acceso no pueda obtener, en una manera de aprendizaje de MAC, la dirección MAC del terminal de usuario o el identificador de interfaz de la interfaz conectada al terminal de usuario, el nodo de conmutación de acceso puede determinar, utilizando un procesador de señal del nodo de conmutación de acceso tal como una unidad CPU o un NP y en una manera de software, el identificador de interfaz de la interfaz que recibe el paquete, aprende satisfactoriamente la dirección MAC del terminal de usuario a partir del paquete enviado por el terminal de usuario y realiza, además, el control sobre el acceso del terminal de usuario utilizando la dirección MAC aprendida del terminal de usuario.

El nodo de conmutación de acceso recibe el paquete enviado por el terminal de usuario que está conectado a la interfaz en el nodo de conmutación de acceso en una manera cableada; encapsula el paquete sobre la base del protocolo para establecer el túnel de transmisión de paquetes; y luego, reenvía el paquete encapsulado al nodo de conmutación de agregación sobre la base del túnel de transmisión de paquetes establecido. A modo de ejemplo, el nodo de conmutación de acceso encapsula, sobre la base del protocolo CAPWAP, el paquete recibido enviado por el terminal de usuario, y luego, envía el paquete encapsulado al nodo de conmutación de agregación.

El nodo de conmutación de agregación recibe el paquete que se envía por el terminal de usuario y reenviado por el nodo de conmutación de acceso, desencapsula el paquete recibido y pone en práctica, en función del paquete desencapsulado, la autenticación de acceso del terminal de usuario que envía el paquete. A modo de ejemplo, cuando el nodo de conmutación de agregación recibe el paquete que está encapsulado sobre la base del protocolo CAPWAP y se transmite por intermedio del túnel de transmisión de paquetes establecido en función del protocolo CAPWAP, el nodo de conmutación de agregación desencapsula también el paquete recibido sobre la base del protocolo CAPWAP y realiza, en conformidad con el paquete desencapsulado, la autenticación sobre el terminal de usuario que envía el paquete. Después de realizar satisfactoriamente la autenticación de acceso en el terminal de usuario, el nodo de conmutación de agregación determina, a partir de la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, el identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, y envía el identificador de interfaz determinado al nodo de conmutación de acceso.

De modo opcional, después de realizar satisfactoriamente la autenticación de acceso sobre el terminal de usuario, el nodo de conmutación de agregación puede determinar, además, un permiso de acceso del terminal de usuario, y enviar el permiso de acceso determinado del terminal de usuario al nodo de conmutación de acceso junto con el identificador de interfaz determinado. El permiso de acceso puede ser uno o más de los permisos de acceso siguientes:

un primer permiso de acceso, que es un permiso del terminal de usuario para acceder a una red de área local virtual (en inglés: virtual local area network, VLAN en forma abreviada), a modo de ejemplo, si una red tiene múltiples redes VLANs, el permiso indica si el terminal de usuario puede acceder a todas las redes VLANs o las redes VLANs que puedan ser específicamente objeto de acceso por el terminal de usuario; y

un segundo permiso de acceso, que consiste en determinar una lista de control de accesos (en inglés: access control list, ACL en forma abreviada) del terminal de usuario.

El nodo de conmutación de acceso recibe el identificador de interfaz enviado por el nodo de conmutación de agregación, determina, en conformidad con el identificador de interfaz recibido, la interfaz que está en el nodo de conmutación de acceso y corresponde al identificador de interfaz, y pone en práctica el control sobre el acceso del terminal de usuario controlando la interfaz determinada. A modo de ejemplo, la etapa anterior puede incluir que el nodo de conmutación de acceso puede activar, en función del identificador de interfaz enviado por el nodo de conmutación de agregación, la interfaz correspondiente al identificador de interfaz recibido, y permitir al terminal de usuario, que está conectado a la interfaz, acceder a una red.

De modo opcional, el nodo de conmutación de agregación determina, en conformidad con el identificador de interfaz recibido, la interfaz que está en el nodo de conmutación de acceso y que corresponde al identificador de interfaz, y realiza el control sobre el acceso del terminal de usuario controlando la interfaz determinada; o puede configurar o

modificar, en conformidad con el permiso de acceso recibido enviado por el nodo de conmutación de agregación, un permiso de acceso de la interfaz que está en el nodo de conmutación de acceso y que corresponde al identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para acceder a una red en conformidad con el permiso de acceso.

El paquete enviado por el terminal de usuario puede ser un paquete 802.1x del Instituto de Ingenieros Eléctricos y Electrónicos (en inglés: Institute of Electrical and Electronics Engineers, IEEE en forma abreviada) u otro tipo de paquete tal como un paquete de Protocolo de Resolución de Dirección (en inglés: Address Resolution Protocol, ARP en forma abreviada) o un paquete de Protocolo de Configuración de Host Dinámico (en inglés: Dynamic Host Configuration Protocol, DHCP en forma abreviada). A continuación se utiliza un paquete IEEE 802.1x a modo de ejemplo para describir, en detalle, las soluciones técnicas dadas a conocer en la forma de realización 1 de la presente invención.

La autenticación de acceso del terminal de usuario se pone en práctica sobre la base del paquete IEEE 802.1x enviado por el terminal de usuario.

En primer lugar, el túnel de transmisión de paquetes que incluye el túnel de control y el túnel de datos se establece a este respecto, sobre la base del protocolo CAPWAP extendido, entre el nodo de conmutación de agregación y el nodo de conmutación de acceso. El túnel de transmisión de paquetes que se establece, sobre la base del protocolo CAPWAP, entre el nodo de conmutación de agregación y el nodo de conmutación de acceso incluye el túnel de control y el túnel de datos. El nodo de conmutación de acceso envía información de atributo del nodo de conmutación de acceso al nodo de conmutación de agregación por intermedio del túnel de control establecido. La información de atributos del nodo de conmutación de acceso incluye un identificador del nodo de conmutación de acceso, a modo de ejemplo, una dirección MAC del nodo de conmutación de acceso, que puede representarse como un conmutador MAC. La información de atributos del nodo de conmutación de acceso puede incluir, además, información de versión de firmware del nodo de conmutación de acceso, que puede representarse como TYPE_SWITCH_VERSION. La información de atributos puede ponerse en práctica extendiendo el elemento de mensaje nº 37 entre los elementos de mensaje en el paquete de control CAPWAP. El elemento de mensaje nº 37 extendido se envía al nodo de conmutación de agregación por intermedio del túnel de control. Un campo de elemento de mensaje en el paquete de control transmitido por intermedio del túnel de control se utiliza para transmitir información de control, en donde el elemento de mensaje puede ser TLVs de diferentes tipos. En el campo de elemento de mensaje, si un valor de T en el TLV es 37, el TLV se utiliza para realizar una extensión del contenido sobre la información de control. En las soluciones técnicas dadas a conocer en la forma de realización 1 de la presente invención, una manera de añadir un nivel 2 TLV al elemento de mensaje en el que se utiliza el valor de T es 37 para realizar la extensión de contenido en el mensaje de control. Más concretamente, el elemento de mensaje en el que el valor de T es 37 puede denominarse como un elemento de mensaje nº 37, en donde un formato estándar del elemento de mensaje nº 37 se ilustra en la tabla 1 anterior.

En segundo lugar, después de que se establezca el túnel de transmisión de paquetes entre el nodo de conmutación de agregación y el nodo de conmutación de acceso sobre la base del protocolo CAPWAP, el nodo de conmutación de agregación mantiene una correspondencia entre el túnel de transmisión de paquetes, que se establece sobre la base del protocolo CAPWAP y un identificador del nodo de conmutación de acceso tal como Switch MAC.

A modo de ejemplo, si se supone que el identificador del nodo de conmutación de acceso es Switch 23, después de que se establezca un túnel de transmisión de paquetes 1 entre el nodo de conmutación de agregación y el nodo de conmutación de acceso cuyo identificador es Switch 23, el nodo de conmutación de agregación puede mantener una correspondencia entre el túnel de transmisión de paquetes 1 y el Switch 23. De este modo, cuando el nodo de conmutación de acceso cuyo identificador es Switch 23 envía un paquete al nodo de conmutación de agregación por intermedio del túnel de transmisión de paquetes establecido posteriormente, y cuando el nodo de conmutación de agregación procesa o responde al paquete, el nodo de conmutación de agregación puede determinar, a partir de la correspondencia mantenida entre el túnel de transmisión de paquetes 1 y Switch 23, un dispositivo que envía el paquete por intermedio del canal de transmisión de paquetes, y un canal de transmisión de paquetes por intermedio del que se transmite información de respuesta al nodo de conmutación de acceso. Más concretamente, el contenido incluido en el elemento de mensaje nº 37 en el paquete de control CAPWAP extendido del nodo de conmutación de acceso puede ser según se ilustra en la tabla 3.

Tabla 3

Tipo de elemento de mensaje: 37, 2 bytes
Longitud de elemento de mensaje: 2 bytes
Identificador del proveedor: un valor de 2011, 4 bytes
Tipo 1 de nivel 2 TLV: TYPE_SWITCH_MAC, 2 bytes
Longitud 1 de nivel 2 TLV: 0x06, 2 bytes

Contenido 1 de nivel 2 TLV: Switch MAC
Longitud 2 de nivel 2 TLV: 0x04, 2 bytes
Contenido 2 de nivel 2 TLV: versión Switch

Para el túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP, el nodo de conmutación de agregación establece una manera de autenticación de cada nodo de conmutación de acceso para la autenticación basada en IEEE 802.1x. A modo de ejemplo, el nodo de conmutación de agregación puede establecer, además, una manera de autenticación de una interfaz en cada nodo de conmutación de acceso según la autenticación basada en la norma IEEE 802.1x.

Cuando se establece una conexión entre el terminal de usuario y la interfaz en el nodo de conmutación de agregación, el nodo de conmutación de acceso recibe el paquete 802.1x enviado por el terminal de usuario, obtiene el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete 802.1x y obtiene la dirección MAC del terminal de usuario a partir del paquete 802.1x recibido enviado por el terminal de usuario. El nodo de conmutación de acceso envía la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de transmisión paquetes establecido sobre la base del protocolo CAPWAP. El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP incluye el túnel de control y el túnel de datos, en donde el túnel de control puede utilizarse para transmitir el paquete de control CAPWAP y el túnel de datos puede utilizarse para transmitir el paquete de datos CAPWAP. De este modo, el nodo de conmutación de acceso puede enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de control.

Más concretamente, el nodo de conmutación de acceso puede enviar, sobre la base del TLV de nivel 2 extendido, la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación, en donde el nivel 2 de TLV extendido se ilustra en la tabla 4. USER_MAC ilustrado en la tabla 4 es la dirección MAC del terminal de usuario, y el índice de interfaz es el identificador de interfaz.

Tabla 4

Tipo de elemento de mensaje: 37, 2 bytes
Longitud de elemento de mensaje: 2 bytes
Identificador del proveedor: un valor de 2011, 4 bytes
Tipo 1 de TLV nivel 2: TYPE_USER_MAC, 2 bytes
Longitud 1 de nivel 2 TLV: 0x06, 2 bytes
Contenido 1 de nivel 2 TLV: USER MAC
Tipo 2 de nivel 2 TLV: TYPE_USER_SWITCH-IF, 2 bytes
Longitud 2 de nivel 2 TLV: 0x04, 2 bytes
Contenido 2 de nivel 2 TLV: índice de interfaz

El nodo de conmutación de acceso captura, en la interfaz del nodo de conmutación de acceso, el paquete 802.1x de IEEE enviado por el terminal de usuario, envía el paquete IEEE 802.1x capturado al nodo de conmutación de agregación por intermedio del canal de transmisión de paquetes establecido sobre la base del protocolo CAPWAP. El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP incluye el túnel de control y el túnel de datos, en donde el túnel de control puede utilizarse para transmitir el paquete de control CAPWAP y el túnel de datos puede utilizarse para transmitir el paquete de datos CAPWAP. Después de la encapsulación del paquete IEEE 802.1x capturado sobre la base del protocolo CAPWAP, el nodo de conmutación de acceso puede enviar el paquete IEEE 802.1x encapsulado al nodo de conmutación de agregación por intermedio del túnel de datos.

El nodo de conmutación de agregación recibe la dirección MAC del terminal de usuario y el identificador de interfaz y mantiene la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz.

En las soluciones técnicas dadas a conocer en la forma de realización 1 de la presente invención, el hecho de que una dirección MAC del terminal de usuario y un identificador de interfaz que es una dirección MAC y un número de interfaz del nodo de conmutación de acceso, se utilicen a modo de ejemplo para la descripción detallada. Un terminal de usuario 1 y un nodo de conmutación de acceso 1 ilustrados en la Figura 2 se utilizan, a modo de ejemplo, para una descripción detallada. Se supone que un identificador del terminal de usuario 1 es UE MAC1, un identificador del nodo de conmutación de acceso 1 es AP MAC1 y el nodo de conmutación de acceso 1 proporciona un total de ocho interfaces de acceso numeradas desde 1 a 8. Si el terminal de usuario 1 está conectado a la

segunda interfaz, el identificador de interfaz de la interfaz es AP MAC1-2. Cuando el terminal de usuario 1 está conectado al nodo de conmutación de acceso 1, el terminal de usuario 1 envía un paquete, y el nodo de conmutación de acceso obtiene el identificador de interfaz AP MAC1-2 de la interfaz conectada al terminal de usuario 1. El nodo de conmutación de acceso 1 captura el paquete enviado por el terminal de usuario 1, utiliza un procesador de señal del nodo de conmutación de acceso 1 para analizar el paquete capturado, para obtener el identificador UE MAC1 del terminal de usuario 1 en el paquete y envía el UE MAC1 obtenido y AP MAC1-2 al nodo de conmutación de agregación por intermedio del túnel de control extendiendo el elemento de mensaje nº 37 en el paquete de control CAPWAP. A modo de ejemplo, el hecho de que el identificador del terminal y el identificador de interfaz que se reciben por el nodo de conmutación de agregación sean respectivamente UE MAC1 y AP MAC1-2 se utiliza a modo de ejemplo para la descripción detallada. El nodo de conmutación de agregación recibe UE MAC1 y AP MAC1-2 que se envían por el nodo de conmutación de acceso, y establece y memoriza una correspondencia entre UE MAC1 y AP MAC1-2.

El nodo de conmutación de acceso recibe el paquete IEEE 802.1x enviado por el terminal de usuario, encapsula el paquete IEEE 802.1x recibido sobre la base del protocolo CAPWAP y luego, envía el paquete encapsulado al nodo de conmutación de agregación por intermedio del túnel de datos.

El nodo de conmutación de agregación recibe el paquete IEEE 802.1x que está encapsulado sobre la base del protocolo CAPWAP, desencapsula el paquete IEEE 802.1x recibido que está encapsulado sobre la base del protocolo CAPWAP, y realiza una autenticación de acceso en conformidad con el paquete IEEE 802.1x desencapsulado.

De modo opcional, el nodo de conmutación de agregación puede limitar, además, la información de permiso del terminal de usuario. Después de que una autenticación satisfactoria, el nodo de conmutación de agregación determina el permiso de acceso del terminal de usuario. El nodo de conmutación de agregación determina, a partir de la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, y envía el identificador de interfaz determinado al nodo de conmutación de acceso.

De modo opcional, el nodo de conmutación de agregación puede enviar, además, el permiso de acceso determinado del terminal de usuario al nodo de conmutación de acceso junto con el identificador de interfaz determinado.

Información tal como la dirección MAC del terminal de usuario, el identificador de interfaz y el permiso de acceso del terminal de usuario pueden enviarse por el nodo de conmutación de agregación al nodo de conmutación de acceso utilizando el nivel 2 de TLV extendido. El nivel 2 de TLV extendido puede ser según se ilustra en la tabla 5. Para un contenido 3 del campo de nivel 2 de TLV en la tabla 5, se utiliza USER VLAN para indicar una red VLAN a la que puede accederse por el terminal de usuario; para un contenido 4 del campo de nivel 2 de TLV, se utiliza un campo de reglas para indicar el permiso de acceso del terminal de usuario.

Tabla 5

Tipo de elemento de mensaje: 37, 2 bytes
Longitud de elemento de mensaje: 2 bytes
Identificador del proveedor: un valor de 2011, 4 bytes
Tipo 1 de nivel 2 TLV: TYPE_USER_MAC, 2 bytes
Longitud 1 de nivel 2 TLV: 0x06, 2 bytes
Contenido 1 de nivel 2 TLV: USER MAC
Tipo 2 de nivel 2 TLV: TYPE_USER_SWITCH_IF, 2 bytes
Longitud 2 de nivel 2 TLV: 0x04, 2 bytes
Contenido 2 de nivel 2 TLV: índice de interfaz
Tipo 3 de nivel 2 TLV: TYPE_USER_VLAN, 2 bytes
Longitud 3 de nivel 2 TLV: 0x02, 2 bytes
Contenido 3 de nivel 2 TLV: USER VLAN
Tipo 4 de nivel 2 TLV: TYPE_USER_ACL, 2 bytes
Longitud 4 de nivel 2 TLV: ampliado, 2 bytes
Contenido 4 de nivel 2 TLV: información de reglas
.....

El nodo de conmutación de acceso determina una interfaz correspondiente en el nodo de conmutación de acceso en conformidad con el identificador de interfaz transmitido en el mensaje de autenticación satisfactoria, activa la interfaz y permite al terminal de usuario acceder a una red.

De modo opcional, el nodo de conmutación de acceso puede controlar, además, en conformidad con el permiso de acceso recibido entregado por el nodo de conmutación de agregación, la interfaz correspondiente al identificador de interfaz, para realizar el control sobre el permiso de acceso del terminal de usuario.

En las soluciones técnicas anteriores dadas a conocer en esta forma de realización de la presente invención, el nodo de conmutación de agregación que tiene una función de reenvío de paquetes se utiliza a modo de ejemplo para una descripción detallada. En la puesta en práctica específica, el controlador dispuesto independientemente en el sistema puede utilizarse, además, para poner en práctica las soluciones técnicas para controlar el acceso del terminal de usuario. Una arquitectura de sistema ilustrada en la Figura 4 incluye al menos un controlador (en inglés: controller) que está dispuesto independientemente, al menos un nodo de conmutación de acceso y al menos un dispositivo de reenvío de paquetes. El dispositivo de reenvío de paquetes puede ser un nodo de conmutación de agregación. El controlador puede conectarse directamente al nodo de conmutación de agregación o puede conectarse al nodo de conmutación de agregación utilizando un enrutador que está dispuesto a este respecto. Cada nodo de conmutación de acceso del al menos un nodo de conmutación de acceso está conectado a un nodo de conmutación de agregación del al menos un nodo de conmutación de agregación. Cualquier nodo de conmutación de acceso del al menos un nodo de conmutación de acceso puede conectarse a al menos un terminal de usuario en una manera cableada, o puede no conectarse a ningún terminal de usuario, es decir, una interfaz utilizada para conexión a un terminal de usuario está en un estado inactivo.

Un túnel de transmisión de paquetes se establece entre el controlador y el nodo de conmutación de acceso. El túnel de transmisión de paquetes entre el controlador el nodo de conmutación de acceso puede establecerse en conformidad con un protocolo propietario prestablecido o extendido un protocolo estándar. El protocolo estándar puede ser el protocolo CAPWAP. En esta forma de realización de la presente invención, el hecho de que un túnel de transmisión de paquetes se establezca extendiendo el protocolo CAPWAP se utiliza a modo de ejemplo para una descripción detallada. El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP extendido incluye un túnel de control para transmitir información de control y túnel de datos para transmitir información de datos.

Después de que se establezca el túnel de transmisión de paquetes sobre la base del protocolo CAPWAP, cuando un terminal de usuario está conectado a una interfaz en el nodo de conmutación de acceso y envía un paquete, el nodo de conmutación de acceso obtiene un identificador de interfaz de la interfaz que recibe el paquete, es decir, un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete; obtiene una dirección MAC del terminal de usuario a partir del paquete recibido; y envía la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al controlador por intermedio del túnel de transmisión de paquetes establecido. El identificador de interfaz de la interfaz en el nodo de conmutación de acceso puede preestablecerse o puede ser una forma de combinación de una identidad de dispositivo del nodo de conmutación de acceso y un número de secuencia de la interfaz.

El nodo de conmutación de acceso puede recibir un paquete enviado por el terminal de usuario conectado a la interfaz en el nodo de conmutación de acceso; determinar, utilizando un procesador de señal del nodo de conmutación de acceso, el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete, extraer un campo de dirección MAC origen del paquete recibido utilizando el procesador de señal, para obtener la dirección MAC del terminal de usuario; y enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de control que está incluido en el túnel de transmisión de paquetes establecido.

El procesador de señal del nodo de conmutación de acceso puede ser una unidad CPU, una combinación de una unidad CPU y un circuito integrado de hardware, un NP, una combinación de una unidad CPU y un NP o una combinación de un NP y un circuito integrado de hardware.

El controlador recibe la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz se envían por el nodo de conmutación de acceso por intermedio del túnel del transmisión de paquetes, y mantiene una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido. La correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz que se mantiene por el controlador puede memorizarse en una manera de memorización intermedia. La correspondencia se memoriza dentro de un período de tiempo; después de que esté terminada la autenticación del acceso realiza en el terminal de usuario, puede suprimirse la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz.

El nodo de conmutación de acceso recibe el paquete enviado por el terminal de usuario que está conectado a la

interfaz en el nodo de conmutación de acceso en una manera cableada; encapsula el paquete sobre la base del protocolo que se utiliza para establecer el túnel de transmisión de paquetes; y luego, reenvía el paquete encapsulado al controlador por intermedio del túnel de transmisión de paquetes establecido. El nodo de conmutación de acceso encapsula, sobre la base del protocolo CAPWAP, el paquete recibido que se envía por el terminal de usuario y luego, envía el paquete encapsulado al controlador.

El controlador recibe el paquete que se envía por el terminal de usuario y reenviado por el nodo de conmutación de acceso, desencapsula el paquete recibido y pone en práctica, en conformidad con el paquete desencapsulado, la autenticación de acceso en el terminal de usuario que envía el paquete. A modo de ejemplo, cuando el controlador recibe el paquete que está encapsulado sobre la base del protocolo CAPWAP y se transmite por intermedio del túnel de transmisión de paquetes establecido sobre la base del protocolo CAPWAP, el controlador desencapsula también el paquete recibido sobre la base del protocolo CAPWAP, y realiza, en conformidad con el paquete desencapsulado, la autenticación sobre el terminal de usuario que envía el paquete. Después de la realización satisfactoria de la autenticación de acceso en el terminal de usuario, el controlador determina, a partir de la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, el identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado y envía el identificador de interfaz determinado al nodo de conmutación de acceso.

De modo opcional, después de la realización satisfactoria de la autenticación de acceso en el terminal de usuario, el controlador puede determinar, además, un permiso de acceso del terminal de usuario y enviar el permiso de acceso determinado del terminal de usuario al nodo de conmutación de acceso junto con el identificador de interfaz determinado. El permiso de acceso puede ser uno o más de los permisos de acceso siguientes:

un primer permiso de acceso, que es un permiso del terminal de usuario para acceder a una red VLAN; a modo de ejemplo, si una red tiene múltiples redes VLANs, el permiso indica si el terminal de usuario puede acceder a todas las redes VLANs o las redes VLANs que puedan ser específicamente objeto de acceso por el terminal de usuario; y

un segundo permiso de acceso, que consiste en determinar una lista ACL del terminal de usuario.

Cuando se recibe el identificador de interfaz enviado por el controlador, el nodo de conmutación de acceso determina, en conformidad con el identificador de interfaz recibido, la interfaz que está en el nodo de conmutación de acceso y que corresponde al identificador de interfaz, y realiza el control sobre el acceso del terminal de usuario controlando la interfaz determinada.

A modo de ejemplo, la etapa anterior puede incluir que el nodo de conmutación de acceso pueda activar, en conformidad con el identificador de interfaz enviado por el nodo de conmutación de agregación, la interfaz correspondiente al identificador de interfaz recibido, y permitir al terminal de usuario, que está conectado a la interfaz, acceder a una red.

De modo opcional, el nodo de conmutación de acceso puede determinar, además, en función del identificador de interfaz recibido, la interfaz que está en el nodo de conmutación de acceso y que corresponde al identificador de interfaz, y realizar el control sobre el acceso del terminal de usuario controlando la interfaz determinada; o puede configurar o modificar, de conformidad con el permiso de acceso recibido enviado por el nodo de conmutación de agregación, un permiso de acceso de la que está en el nodo de conmutación de acceso y que corresponde al identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para acceder a una red de conformidad con el permiso de acceso. El paquete enviado por el terminal de usuario puede ser un paquete IEEE 802.1x u otro tipo de paquete tal como un paquete ARP o un paquete DHCP.

Forma de realización 2

Sobre la base de la arquitectura del sistema ilustrada en la Figura 2, la forma de realización 2 de la presente invención da a conocer un método para controlar el acceso de un terminal de usuario. Según se ilustra en la Figura 5, un procedimiento de procesamiento específico del método es como sigue:

Etapa 51: Establecer un túnel de transmisión de paquetes entre un nodo de conmutación de acceso y un nodo de conmutación de agregación.

El túnel de transmisión de paquetes entre el nodo de conmutación de agregación y el nodo de conmutación de acceso puede establecerse en conformidad con un protocolo propietario prestablecido o extendiendo un protocolo estándar. A modo de ejemplo, el protocolo estándar puede ser un protocolo CAPWAP. En la forma de realización 2 de la presente invención, el hecho de que el túnel de transmisión de paquetes se establezca extendiendo el protocolo CAPWAP se utiliza, a modo de ejemplo, para una descripción detallada. El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP extendido incluye un túnel de control para transmitir información de control y un túnel de datos para transmitir información de datos.

Etapa 52: El nodo de conmutación de acceso obtiene una dirección MAC de un terminal de usuario conectado a una interfaz en el nodo de conmutación de acceso y un identificador de interfaz de la interfaz conectada al terminal de usuario.

El terminal de usuario está conectado a la interfaz en el nodo de conmutación de acceso en una manera cableada, y envía un paquete.

Cuando el terminal de usuario está conectado a la interfaz en el nodo de conmutación de acceso y envía un paquete, el nodo de conmutación de acceso obtiene el identificador de interfaz de la interfaz conectada al terminal de usuario, captura el paquete enviado por el terminal de usuario, obtiene la dirección MAC del terminal de usuario a partir del paquete capturado, y envía la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de transmisión de paquetes establecido. El identificador de interfaz de la interfaz en el nodo de conmutación de acceso puede preestablecerse, o puede ser una forma de combinación de una identidad de dispositivo del nodo de conmutación de acceso y un número de secuencia de la interfaz. El nodo de conmutación de acceso puede recibir un paquete enviado por el terminal de usuario conectado a la interfaz en el nodo de conmutación de acceso; determinar, utilizando un procesador de señal del nodo de conmutación de acceso, el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete; extraer un campo de dirección MAC origen del paquete recibido utilizando el procesador de señal, para obtener la dirección MAC del terminal de usuario; y enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de control que está incluido en el túnel de transmisión de paquetes establecido.

El procesador de señal del nodo de conmutación de acceso puede ser una unidad CPU, una combinación de una CPU y un circuito integrado de hardware, un NP, una combinación de una CPU y un NP, o una combinación de un NP y un circuito integrado de hardware.

El paquete que se envía por el terminal de usuario y se captura por el nodo de conmutación de acceso puede incluir paquete IEEE 802.1x, un paquete ARP o un paquete DHCP.

Etapa 53: El nodo de conmutación de acceso envía el identificador de interfaz obtenido y la dirección MAC obtenida del terminal de usuario al nodo de conmutación de agregación por intermedio del túnel de transmisión de paquetes establecido.

El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP incluye el túnel de control y el túnel de datos, en donde el túnel de control puede utilizarse para transmitir un paquete de control y el túnel de datos puede utilizarse para transmitir un paquete de datos. De este modo, el nodo de conmutación de acceso puede enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de control. El nodo de conmutación de acceso puede enviar, sobre la base del nivel 2 de TLV extendido, la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación. El nivel 2 de TLV extendido se describe en la tabla 4 anterior.

Etapa 54: El nodo de conmutación de agregación recibe la dirección MAC del terminal de usuario y el identificador de interfaz que se envía por el nodo de conmutación de acceso, y mantiene una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz.

La correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz que se mantiene por el nodo de conmutación de agregación puede memorizarse en una manera de memorización intermedia. La correspondencia se memoriza dentro de un período de tiempo; después de que se termine la autenticación de acceso realizada en el terminal de usuario, puede suprimirse la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz.

Etapa 55: El nodo de conmutación de acceso captura, en la interfaz del nodo de conmutación de acceso, un paquete enviado por el terminal de usuario y envía el paquete capturado al nodo de conmutación de agregación por intermedio del canal de transmisión de paquetes establecido sobre la base del protocolo CAPWAP.

El túnel de transmisión de paquetes que se establece sobre la base del protocolo CAPWAP incluye el túnel de control y el túnel de datos, en donde el túnel de control puede utilizarse para transmitir un paquete de control y el túnel de datos puede utilizarse para transmitir un paquete de datos. El nodo de conmutación de acceso puede encapsular el paquete capturado sobre la base del protocolo CAPWAP y luego, enviar el paquete encapsulado al nodo de conmutación de agregación por intermedio del túnel de datos.

Etapa 56: El nodo de conmutación de agregación recibe el paquete que se envía por intermedio del túnel de transmisión de paquetes, desencapsula el paquete recibido, obtiene la dirección MAC del terminal de usuario y realiza la autenticación de acceso en el terminal de usuario.

El nodo de conmutación de agregación recibe el paquete encapsulado sobre la base del protocolo CAPWAP, desencapsula el paquete recibido que está encapsulado sobre la base del protocolo CAPWAP y realiza la autenticación de acceso en conformidad con el paquete desencapsulado.

Una manera específica de puesta en práctica de la autenticación de acceso en el terminal es la misma que la autenticación de acceso común y sus detalles no se describen de nuevo en esta forma de realización de la presente invención.

Etapa 57: Después de una autenticación satisfactoria, el nodo de conmutación de agregación determina, a partir de la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, el identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado y envía el identificador de interfaz determinado al terminal de usuario.

De modo opcional, después de la realización satisfactoria de la autenticación de acceso sobre el terminal de usuario, el nodo de conmutación de agregación puede determinar, además, un permiso de acceso del terminal de usuario y envía el permiso de acceso determinado del terminal de usuario al nodo de conmutación de acceso junto con el identificador de interfaz determinado.

Un mensaje de autenticación satisfactoria enviado por el nodo de conmutación de agregación al nodo de conmutación de acceso puede incluir información tal como la dirección MAC del terminal de usuario, el identificador de interfaz y el permiso de acceso del terminal de usuario y la información puede enviarse al nodo de conmutación de acceso utilizando el nivel 2 de TLV extendido. El nivel 2 de TLV extendido puede ser según se describió en la tabla 5 anterior.

Etapa 58: El nodo de conmutación de acceso recibe el identificador de interfaz enviado por el nodo de conmutación de agregación, activa la interfaz correspondiente al identificador de interfaz y realiza el control sobre el acceso del terminal de usuario controlando la interfaz determinada.

A modo de ejemplo, el nodo de conmutación de acceso puede activar, en conformidad con el identificador de interfaz enviado por el nodo de conmutación de agregación, la interfaz correspondiente al identificador de interfaz recibido, y permitir al terminal de usuario, que está conectado a la interfaz, acceder a una red para la transmisión de paquetes.

De modo opcional, el nodo de conmutación de acceso puede recibir, además, el permiso de acceso que está en correspondencia con el terminal de usuario y se envía por el nodo de conmutación de agregación; y realizar el control, controlando la interfaz conectada al terminal de usuario, el terminal de usuario para acceder a una red en conformidad con el permiso de acceso recibido.

El paquete enviado por el terminal de usuario puede ser un paquete IEEE 802.1x u otro tipo de paquete tal como un paquete ARP o un paquete DHCP.

El diagrama de flujo del método para controlar el acceso de un terminal de usuario ilustrado en la Figura 5 y el método anterior para controlar el acceso de un terminal de usuario dado a conocer en la forma de realización 2 de la presente invención son simplemente maneras de puesta en práctica preferidas descritas en esta forma de realización de la presente invención. En una puesta en práctica específica, puede realizarse un procesamiento alternativo en conformidad con el procedimiento del método anterior.

Forma de realización 3

En consecuencia, sobre la base de la arquitectura de sistema ilustrada en la Figura 2 y para un nodo de conmutación de agregación, una forma de realización de la presente invención da a conocer un método para controlar el acceso de un terminal de usuario. Según se ilustra en la Figura 6a, un procedimiento de procesamiento específico del método es como sigue:

Etapa 61: Establecer, entre el nodo de conmutación de agregación y el nodo de conmutación de acceso, un túnel de transmisión de paquetes que incluye un túnel de control y un túnel de datos.

El nodo de conmutación de agregación puede establecer el túnel de transmisión de paquetes con el nodo de conmutación de acceso sobre la base de un protocolo propietario o sobre la base de la extensión de un protocolo estándar. En la forma de realización 3 de la presente invención, el túnel de transmisión de paquetes se establece entre el controlador y el nodo de conmutación de acceso sobre la base de la extensión del protocolo CAPWAP.

Para un proceso de establecer el túnel de transmisión de paquetes sobre la base del protocolo CAPWAP, puede hacerse referencia a la descripción detallada en la forma de realización 1 y por ello, los detalles no se describen de nuevo en la forma de realización 3 de la presente invención.

Durante un proceso de establecimiento del túnel de transmisión de paquetes entre el nodo de conmutación de agregación y el nodo de conmutación de acceso sobre la base del protocolo CAPWAP, el nodo de conmutación de agregación mantiene una correspondencia entre el túnel de transmisión de paquetes establecido y el nodo de conmutación de acceso. A modo de ejemplo, se supone que el identificador del nodo de conmutación de acceso es Switch 23, después de que se establezca el túnel de transmisión de paquetes 1 establecido entre el nodo de conmutación de agregación y el nodo de conmutación de acceso cuyo identificador es Switch 23, el nodo de conmutación de agregación puede mantener una correspondencia entre el túnel de transmisión de paquetes 1 y Switch 23. De este modo, cuando el nodo de conmutación de acceso cuyo identificador es Switch 23 envía un paquete al nodo de conmutación de agregación por intermedio del túnel de transmisión de paquetes establecido con posterioridad, y cuando el nodo de conmutación de agregación procesa o responde al paquete, el nodo de conmutación de agregación puede determinar, a partir de la correspondencia mantenida entre el túnel de transmisión de paquetes 1 y Switch 23, un dispositivo que envía el paquete, un canal de transmisión de paquetes por el que se envía el paquete, un nodo de conmutación de acceso al que ha de transmitirse el paquete y un canal de transmisión de paquetes por intermedio del cual se transmitirá la información de respuesta.

Etapa 62: El nodo de conmutación de agregación recibe un paquete de autenticación enviado por el nodo de conmutación de acceso por intermedio del túnel de datos establecido.

El paquete enviado por el nodo de conmutación de acceso es un paquete que se envía por el terminal de usuario conectado a una interfaz en el nodo de conmutación de acceso y se captura en la interfaz por el nodo de conmutación de acceso. El paquete capturado se envía al nodo de conmutación de agregación después de ser encapsulado sobre la base del protocolo CAPWAP. El paquete capturado por el nodo de conmutación de acceso puede ser un paquete 802.1x, un paquete ARP o un paquete DHCP.

Etapa 63: El nodo de conmutación de agregación obtiene una dirección MAC en un campo de dirección MAC origen del paquete de autenticación y realiza la autenticación de acceso en un terminal de usuario que corresponde a la dirección MAC obtenida.

Etapa 64: Después de que se realice la autenticación de acceso satisfactoriamente en el terminal de usuario, a partir de una correspondencia mantenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado.

Una correspondencia entre una dirección MAC de un terminal de usuario y un identificador de interfaz del nodo de conmutación de acceso conectado al terminal de usuario puede determinarse en la manera siguiente: recibir la dirección MAC del terminal de usuario que se envía por el nodo de conmutación de acceso por intermedio del túnel de control y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario se obtiene por el nodo de conmutación de acceso cuando el terminal de usuario establece una conexión con la interfaz en el nodo de conmutación de acceso, y envía un paquete por intermedio de la interfaz conectada; y establecer una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido.

La correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz que se mantiene por el nodo de conmutación de agregación puede memorizarse en una manera de memorización instantánea. La correspondencia se memoriza dentro de un período de tiempo; después de que la autenticación de acceso realizada en el terminal de usuario esté completa, se puede suprimir la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz. Más concretamente, para el establecimiento de la correspondencia entre una dirección MAC de un terminal de usuario y un identificador de interfaz, puede hacerse referencia a la descripción detallada en la forma de realización 1 y la forma de realización 2, y los detalles no se describen, de nuevo, en la forma de realización 3 de la presente invención.

Etapa 65: Enviar el identificador de interfaz determinado al nodo de conmutación de acceso por intermedio del túnel de control establecido entre el controlador y el nodo de conmutación de acceso y dar instrucciones al nodo de conmutación de acceso para activar la interfaz que corresponde al identificador de interfaz.

De modo opcional, la autenticación de acceso realizada en el terminal de usuario puede incluir, además, la determinación de un permiso de acceso del terminal de usuario. El nodo de conmutación de agregación envía el permiso de acceso determinado del terminal de usuario al nodo de conmutación de acceso por intermedio del túnel de control, da instrucciones al nodo de conmutación de acceso para controlar, en conformidad con el permiso de acceso, el terminal de usuario para pasar a través del identificador de interfaz.

En correspondencia, la forma de realización 3 de la presente invención da a conocer, además, un aparato para controlar el acceso de un terminal de usuario. Según se ilustra en la Figura 6b, el aparato incluye:

un módulo de recepción 701, configurado para: recibir un paquete de autenticación enviado por intermedio de un túnel de datos establecido y transmitir el paquete de autenticación recibido a un módulo de obtención 702;

el módulo de obtención 702, configurado para: obtener el paquete de autenticación transmitido por el módulo de recepción 701, obtener una dirección MAC en un campo de dirección MAC origen del paquete de autenticación, y transmitir la dirección MAC obtenida a un módulo de autenticación 703;

el módulo de autenticación 703, configurado para: recibir la dirección MAC transmitida por el módulo de obtención 702, realizar la autenticación de acceso sobre el terminal de usuario que corresponde a la dirección MAC y transmitir un resultado de la autenticación satisfactoria a un módulo de determinación 704;

el módulo de determinación 704, configurado para: obtener el resultado de la autenticación satisfactoria que se transmite por el módulo de autenticación 703, determinar, a partir de una correspondencia mantenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, en donde el identificador de interfaz es un identificador de interfaz de una interfaz en un nodo de conmutación de acceso conectado al terminal de usuario; y transmitir el identificador de interfaz a un módulo de envío 705; y

el módulo de envío 705, configurado para: obtener el identificador de interfaz transmitido por el módulo de determinación 704, enviar el identificador de interfaz determinado al nodo de conmutación de acceso por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso y dar instrucciones al nodo de conmutación de acceso para activar la interfaz correspondiente al identificador de interfaz.

El módulo de recepción anterior 701 está configurado, además, para: recibir la dirección MAC del terminal de usuario enviada por el nodo de conmutación de acceso por intermedio del túnel de control y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso que se conecta al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario se obtienen por el nodo de conmutación de acceso cuando el terminal de usuario establece una conexión con la interfaz en el nodo de conmutación de acceso, y envía un paquete por intermedio de la interfaz conectada; y transmitir la dirección MAC recibida en el identificador de interfaz recibido a un módulo de establecimiento 706.

El aparato comprende, además, el módulo de establecimiento 706, configurado para: obtener la dirección MAC y el identificador de interfaz que se transmiten por el módulo de recepción 705, y establecer una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido.

En correspondencia, la forma de realización 3 de la presente invención da a conocer, además, un conmutador de red. Según se ilustra en la Figura 6c, el conmutador de red incluye: una interfaz 801, una memoria 803 y un procesador de señal 804.

La interfaz 801 está configurada para: recibir un paquete de autenticación enviado por intermedio de túnel de datos establecido y transmitir el paquete de autenticación recibido al procesador de señal 804 por intermedio de un bus de conexión 802.

La interfaz 801 puede ser una o más de entre: un controlador de interfaz de red (en inglés: network interface controller, NIC en forma abreviada) que proporciona una interfaz cableada, a modo de ejemplo, un NIC de Ethernet que puede proporcionar una interfaz cableada de cobre y/o una interfaz de fibra; un NIC que proporciona una interfaz inalámbrica, a modo de ejemplo, un NIC de red de área local inalámbrica (en inglés: wireless local area network, WLAN en forma abreviada).

La memoria 803 está configurada para: memorizar un código de programa y memorizar una correspondencia entre una dirección MAC de un terminal de usuario y un identificador de interfaz, y transmitir el código de programa memorizado al procesador de señal 804 por intermedio del bus de conexión 802.

La memoria 803 puede ser una memoria volátil (en inglés: volatile memory), a modo de ejemplo, una memoria de acceso aleatorio (en inglés: random-access memory, RAM en forma abreviada); o una memoria no volátil (en inglés: non-volatile memory), a modo de ejemplo, una memoria instantánea (en inglés: flash memory), una unidad de disco duro (en inglés: hardware disk drive, HDD en forma abreviada) o una unidad de estado sólido (en inglés: solid-state drive, SSD en forma abreviada) o una combinación de memorias de los tipos anteriores.

El procesador de señal 804 está configurado para: obtener, utilizando el bus 802, el código de programa memorizado en la memoria 803 y ejecutar lo que sigue de conformidad con el código de programa obtenido: obtener la dirección MAC en un campo de dirección MAC origen del paquete de autenticación; realizar una autenticación de acceso sobre el terminal de usuario correspondiente a la dirección MAC; después de una autenticación satisfactoria de acceso, obtener la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz

que se memorizan en la memoria 803; determinar, a partir de la correspondencia obtenida entre la dirección MAC del terminal de usuario y el identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, en donde el identificador de interfaz es un identificador de interfaz de la interfaz en un nodo de conmutación de acceso conectado al terminal de usuario; y transmitir el identificador de interfaz a la interfaz 801 por intermedio del bus de conexión 802.

El procesador de señal 804 puede ser una unidad central de procesamiento (en inglés: central processing unit, CPU en forma abreviada), una combinación de una unidad CPU y un circuito integrado de hardware, un procesador de red (en inglés: network processor, NP en forma abreviada), una combinación de una CPU y un NP o una combinación de un NP y un circuito integrado de hardware.

El circuito integrado de hardware anterior puede ser uno o una combinación de los circuitos integrados siguientes: un circuito integrado específico de la aplicación (en inglés: application-specific integrated circuit, ASIC en forma abreviada), un conjunto matricial de puertas electrónicas programables in situ (en inglés: field-programmable gate array, FPGA en forma abreviada) y un dispositivo lógico programable complejo (en inglés: complex programmable logic device, CPLD en forma abreviada).

La interfaz anterior 801 está configurada, además, para: obtener, utilizando el bus 802, el identificador de interfaz transmitido por el procesador de señal 804, enviar el identificador de interfaz determinado al nodo de conmutación de acceso por intermedio del túnel de control establecido entre el controlador y el nodo de conmutación de acceso, y dar instrucciones al nodo de conmutación de acceso para activar la interfaz correspondiente al identificador de interfaz.

La interfaz anterior 801 está configurada, además, para: recibir la dirección MAC del terminal de usuario enviada por el nodo de conmutación de acceso por intermedio del túnel de control, y el identificador de interfaz de una interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario se obtienen por el nodo de conmutación de acceso cuando el terminal de usuario establece una conexión con la interfaz en el nodo de conmutación de acceso, y envía un paquete por intermedio de la interfaz conectada; y transmitir la dirección MAC recibida y el identificador de interfaz recibido al procesador de señal 804 por el intermedio del bus de conexión.

El procesador de señal 804 está configurado, además, para: obtener, utilizando el bus de conexión 802, la dirección MAC y el identificador de interfaz que se transmiten por la interfaz 801; establecer una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC del terminal de usuario y el identificador de interfaz recibido; y transmitir la correspondencia establecida entre la dirección MAC y el identificador de interfaz a la memoria 803 por intermedio del bus 802.

En correspondencia, sobre la base de la arquitectura del sistema ilustrada en la Figura 2 y para un nodo de conmutación de acceso, la forma de realización 3 de la presente invención da a conocer un método para controlar el acceso de un terminal de usuario. Según se ilustra en la Figura 7a, un procedimiento de procesamiento específico del método es como sigue:

Etapa 71: Establecer, entre el nodo de conmutación de acceso y un nodo de conmutación de agregación, un túnel de transmisión de paquetes que incluye un túnel de control y un túnel de datos.

El nodo de conmutación de agregación puede establecer el túnel de transmisión de paquetes con el nodo de conmutación de acceso sobre la base de un protocolo propietario o sobre la base de la extensión de protocolo estándar. En la forma de realización 3 de la presente invención, el túnel de transmisión de paquetes se establece entre el controlador y el nodo de conmutación de acceso sobre la base de la extensión del protocolo CAPWAP.

Para un proceso de establecer el túnel de transmisión de paquetes sobre la base del protocolo CAPWAP, puede hacerse referencia a la descripción detallada en la forma de realización 1 y los detalles no se describen de nuevo en la forma de realización 3 de la presente invención.

Durante un proceso de establecimiento del túnel de transmisión de paquetes entre el nodo de conmutación de agregación y el nodo de conmutación de acceso sobre la base del protocolo CAPWAP, el nodo de conmutación de agregación mantiene una correspondencia entre el túnel de transmisión de paquetes establecido y el nodo de conmutación de acceso. A modo de ejemplo, se supone que el identificador del nodo de conmutación de acceso es Switch 23, después de que se establezca un túnel de transmisión de paquetes 1 entre el nodo de conmutación de agregación y el nodo de conmutación de acceso cuyo identificador es Switch 23, el nodo de conmutación de agregación puede mantener una correspondencia entre el túnel de transmisión de paquetes 1 y Switch 23. De este modo, cuando el nodo de conmutación de acceso cuyo identificador es Switch 23 envía un paquete al nodo de conmutación de agregación por intermedio del túnel de transmisión de paquetes establecido con posterioridad, y cuando el nodo de conmutación de agregación procesa o responde al paquete, el nodo de conmutación de agregación puede determinar, a partir de la correspondencia mantenida entre el túnel de transmisión de paquetes 1

y Switch 23, un dispositivo que envía el paquete, un canal de transmisión de paquetes a través del cual se envía el paquete, un nodo de conmutación de acceso al que ha de transmitirse el paquete y un canal de transmisión de paquetes por intermedio del cual se transmitirá la información de respuesta.

Etapa 72: Cuando se desactiva una función de aprendizaje de control de acceso al soporte MAC, el nodo de conmutación de acceso recibe un paquete de autenticación enviado por un terminal de usuario que está conectado a una interfaz en el nodo de conmutación de acceso.

Etapa 73: Obtener un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido.

El nodo de conmutación de acceso determina, utilizando un procesador de señal que es capaz de realizar una función de procesamiento de conformidad con un código de programa, el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y transmite el paquete de autenticación recibido al procesador de señal del nodo de conmutación de acceso; y el procesador de señal obtiene, a partir de un campo de dirección MAC origen del paquete de autenticación, la dirección MAC del terminal de usuario que envía el paquete de autenticación.

Etapa 74: Enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido al nodo de conmutación de agregación por intermedio del túnel de control establecido.

Etapa 75: Recibir el identificador de interfaz enviado por el nodo de conmutación de agregación por intermedio del túnel de control y activar, en conformidad con el identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz.

El identificador de interfaz es un identificador de interfaz que está determinado, después de que el nodo de conmutación de agregación realice satisfactoriamente la autenticación de acceso en el terminal de usuario, a partir de la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario y que corresponde a la dirección MAC del terminal de usuario satisfactoriamente autenticado.

Para una manera de puesta en práctica específica de establecer, por el nodo de conmutación de agregación, la correspondencia entre el identificador del terminal y el identificador de interfaz, puede hacerse referencia a la descripción detallada en la forma de realización 1 o la forma de realización 2, y los detalles no se describen de nuevo en la forma de realización 3 de la presente invención.

De modo opcional, el nodo de conmutación de acceso recibe un permiso de acceso que es del terminal de usuario correspondiente a la dirección MAC y se envía por el controlador por intermedio del túnel de control; y configura o modifica, en conformidad con el permiso de acceso recibido enviado por el nodo de conmutación de agregación, el permiso de acceso de la interfaz que está en el nodo de conmutación de acceso y está en correspondencia con el identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para acceder a una red en conformidad con el permiso de acceso.

En correspondencia, la forma de realización 3 de la presente invención da a conocer, además, un aparato para controlar el acceso de un terminal de usuario. Según se ilustra en la Figura 7b, el aparato incluye:

un módulo de recepción 901, configurado para: cuando se desactiva una función de aprendizaje de control de acceso al soporte MAC, recibir un paquete de autenticación enviado por un terminal de usuario que está conectado a una interfaz en el nodo de conmutación de acceso, y transmitir el paquete de autenticación a un módulo de obtención 902;

el módulo de obtención 902, configurado para: recibir el paquete de autenticación transmitido por el módulo de recepción 901, obtener un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido y transmitir el identificador de interfaz y la dirección MAC a un módulo de envío 903;

el módulo de envío 903, configurado para: recibir el identificador de interfaz y la dirección MAC que se transmiten por el módulo de obtención 902 y enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido a un controlador por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, de modo que el controlador mantenga una correspondencia entre la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido; en donde

el módulo de recepción anterior 901, está configurado, además, para: recibir el identificador de interfaz enviado por el controlador por intermedio del túnel de control y transmitir el identificador de interfaz a un módulo de control 904, en donde el identificador de interfaz es un identificador de interfaz que se determina a partir de la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz después de que el controlador realice, de

forma satisfactoria, la autenticación de acceso en el terminal de usuario que corresponde a la dirección MAC y que corresponde a la dirección MAC del terminal de usuario satisfactoriamente autenticado; y

el módulo de control 904, configurado para: obtener el identificador de interfaz transmitido por el módulo de recepción 901 y activar, en conformidad con el identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz.

Más concretamente, el módulo de recepción anterior 901 está configurado, además, para: recibir un permiso de acceso que es del terminal de usuario correspondiente a la dirección MAC y se envía por el controlador por intermedio del túnel de control, y transmitir el permiso de acceso al módulo de control; y el módulo de control 904 está específicamente configurado para: obtener el permiso de acceso transmitido por el módulo de recepción 901, y configurar o modificar, en conformidad con un permiso de acceso recibido enviado por un nodo de conmutación de agregación, el permiso de acceso de la interfaz que está en el nodo de conmutación de acceso y que corresponde al identificador de interfaz, para controlar el terminal de usuario, que se conecta a la interfaz, para acceder a una red en conformidad con el permiso de acceso.

Más concretamente, el módulo de obtención anterior 902 incluye concretamente un procesador de señal, y está configurado para: determinar el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y obtener el paquete de autenticación transmitido por el módulo de recepción; y el procesador de señal obtiene, a partir de un campo de dirección MAC origen del paquete de autenticación, la dirección MAC del terminal de usuario que envía el paquete de autenticación.

En correspondencia, la forma de realización 3 de la presente invención da a conocer, además, un conmutador de red. Según se ilustra en la Figura 7c, el conmutador de red incluye: una interfaz 101 y un procesador de señal 103.

La interfaz 101 está configurada para: cuando se desactiva una función de aprendizaje de control de acceso al soporte MAC, recibir un paquete de autenticación enviado por un terminal de usuario que está conectado a una interfaz en el nodo de conmutación de acceso, y transmitir el paquete de autenticación al procesador de señal 103 por intermedio de un bus 102.

La interfaz 101 puede ser una o más de entre: un NIC que proporciona una interfaz cableada, a modo de ejemplo, un NIC de Ethernet que puede proporcionar una interfaz cableada de cobre y/o una interfaz de fibra.

El procesador de señal 103 está configurado para: recibir, por intermedio del bus 102, el paquete de autenticación transmitido por la interfaz 101, obtener un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el mensaje de autenticación, obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido y transmitir el identificador de interfaz y la dirección MAC a la interfaz 101 por intermedio del bus 102.

El procesador de señal 103 puede ser una unidad CPU, una combinación de una CPU y un circuito integrado de hardware, un NP, una combinación de una CPU y un NP o una combinación de un NP y un circuito integrado de hardware.

El circuito integrado de hardware anterior puede ser uno o una combinación de los circuitos integrados siguientes: ASIC, FPGA, CPLD y similares.

De modo opcional, en un caso en el que el procesador de señal 103 es una unidad CPU o una combinación de componentes que incluyen una CPU, un dispositivo de retransmisión puede incluir, además, una memoria, en donde la memoria está configurada para memorizar un código de programa. El procesador de señal obtiene el código de programa memorizado a partir de la memoria y realiza el procesamiento correspondiente en función del código de programa obtenido.

La memoria puede ser una memoria volátil, a modo de ejemplo, una memoria de acceso aleatorio; o una memoria no volátil, a modo de ejemplo, una memoria de solamente lectura (en inglés: read-only memory, ROM en forma abreviada), una memoria instantánea, una unidad de disco duro o una unidad de estado sólido; o una combinación de las memorias de los tipos anteriores.

La interfaz anterior 101 está configurada, además, para: recibir, por intermedio del bus 102, el identificador de interfaz y la dirección MAC que se transmiten por el procesador de señal 103 y enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido a un controlador por intermedio de un túnel de control establecido, de modo que el controlador mantenga una correspondencia entre la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido.

La interfaz anterior 101 está configurada, además, para: recibir el identificador de interfaz enviado por el controlador por intermedio del túnel de control, y transmitir el identificador de interfaz al procesador de señal 103 por intermedio del bus 102, en donde el identificador de interfaz es un identificador de interfaz que se determina a partir de la

correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz después de que el controlador realice, de forma satisfactoria, la autenticación de acceso del terminal de usuario correspondiente a la dirección MAC y corresponde a la dirección MAC del terminal de usuario satisfactoriamente autenticado.

El procesador de señal 103 está configurado para: obtener, utilizando el bus 102, el identificador de interfaz transmitido por la interfaz 101 y activar, en conformidad con el identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz.

Más concretamente, la interfaz 101 está configurada, además, para: recibir un permiso de acceso que es del terminal de usuario correspondiente a la dirección MAC y se envía por el controlador por intermedio del túnel de control, y transmitir el permiso de acceso al procesador de señal 103 por intermedio del bus 102. El procesador de señal 103 está específicamente configurado para: obtener el permiso de acceso transmitido por la interfaz 101 por intermedio del bus 102 y configurar o modificar, en conformidad con el permiso de acceso recibido, el permiso de acceso de la interfaz que está en el nodo de conmutación de acceso y que corresponde al identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para acceder a una red en conformidad con el permiso de acceso.

Más concretamente, el procesador de señal anterior 103 está configurado para: determinar el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y obtener el paquete de autenticación transmitido por la interfaz 101; y el procesador de señal 103 obtiene, a partir del campo de dirección MAC origen del paquete de autenticación, la dirección MAC del terminal de usuario que envía el paquete de autenticación.

En las soluciones técnicas dadas a conocer en las formas de realización de la presente invención, un control centralizado sobre el acceso de terminales de usuario puede realizarse en un nodo de conmutación de agregación y el control de política distribuido puede realizarse en un nodo de conmutación de acceso, para controlar las funciones de reenvío de datos de terminales de usuario en una capa de acceso mientras se realiza una gestión centralizada de los terminales de usuario. De este modo, una manera de puesta en práctica es relativamente fácil, una arquitectura de sistema es relativamente simple y la seguridad de la red se puede mejorar todavía más.

Un experto en esta técnica debe entender que las formas de realización de la presente invención pueden proporcionarse como un método, un aparato (dispositivo) o un producto de programa informático. Por lo tanto, la presente invención puede utilizar una forma de realización solamente de hardware, solamente de software o formas de realización con una combinación de software y hardware. Además, la presente invención puede utilizar una forma de un producto de programa informático que se pone en práctica en uno o más soportes de memorización utilizables por ordenador (incluyendo, sin limitación, una memoria de disco, una memoria de solamente lectura óptica, una memoria óptica y similares) que incluyen un código de programa utilizable por ordenador.

La presente invención se describe con referencia a los diagramas de flujo y/o diagramas de bloque del método, el aparato (dispositivo) y el producto de programa informático en conformidad con las formas de realización de la presente invención. Debe entenderse que las instrucciones del programa informático pueden utilizarse para realizar cada procedimiento y/o cada bloque en los diagramas de flujo y/o los diagramas de bloques y una combinación de un procedimiento y/o un bloque en los diagramas de flujo y/o los diagramas de bloques. Estas instrucciones de programa informático pueden proporcionarse para un ordenador de uso general, un ordenador especializado, un procesador incorporado o un procesador de cualquier otro dispositivo de procesamiento de datos programable para generar una máquina, de modo que las instrucciones ejecutadas por un ordenador o un procesador de cualquier otro dispositivo de procesamiento de datos programable generan un aparato para realizar una función especificada en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Las instrucciones de programa informático pueden memorizarse también en una memoria legible por ordenador que puede dar instrucciones al ordenador o a cualquier dispositivo de procesamiento de datos programable para trabajar de una manera específica, de modo que las instrucciones memorizadas en la memoria legible por ordenador generen un artefacto informático que incluya un aparato de instrucción. El aparato de instrucción realiza una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático pueden cargarse también en un ordenador u otro dispositivo de procesamiento de datos programable, de modo que una serie de operaciones y etapas se realicen en el ordenador o el otro dispositivo programable, con lo que se genera un procesamiento realizado por ordenador. En consecuencia, las instrucciones ejecutadas en el ordenador o el otro dispositivo programable proporcionan etapas para realizar una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Aunque algunas formas de realización preferidas de la presente invención han sido descritas, los expertos en esta técnica pueden realizar cambios y modificaciones a estas formas de realización una vez que asimilen el concepto inventivo básico. Por lo tanto, las siguientes reivindicaciones están previstas para interpretarse como que cubren las

formas de realización preferidas y todos los cambios y modificaciones que caigan dentro del alcance de la presente invención.

5

REIVINDICACIONES

1. Un método para controlar el acceso de un terminal de usuario, que comprende:

recibir (62), por un controlador, un paquete de autenticación enviado por un nodo de conmutación de acceso por intermedio de un túnel de datos establecido;

obtener (63), por el controlador, una dirección de control de acceso al soporte, MAC, en un campo de dirección MAC origen del paquete de autenticación;

después de que se ponga en práctica, de forma satisfactoria, una autenticación de acceso en un terminal de usuario correspondiente a la dirección MAC obtenida, determinar (64), a partir de una correspondencia mantenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, en donde el identificador de interfaz es un identificador de interfaz de una interfaz en el nodo de conmutación de acceso conectado al terminal de usuario; y

enviar (65), por el controlador, el identificador de interfaz determinado al nodo de conmutación de acceso por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, y dar instrucciones al nodo de conmutación de acceso para permitir la activación de la interfaz correspondiente al identificador de interfaz.

2. El método según la reivindicación 1, antes de que se ponga en práctica la autenticación de acceso en el terminal de usuario correspondiente a la dirección MAC, la correspondencia entre una dirección MAC de un terminal de usuario y un identificador de interfaz se determina en la manera siguiente:

recibir, por el controlador, la dirección MAC del terminal de usuario enviada por el nodo de conmutación de acceso por intermedio del túnel de control, y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario se obtiene por el nodo de conmutación de acceso cuando el terminal de usuario establece una conexión con la interfaz en el nodo de conmutación de acceso, y enviar un paquete por intermedio de la interfaz conectada; y

establecer una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido.

3. Un método para controlar el acceso de un terminal de usuario, que comprende:

cuando se desactiva una función de aprendizaje de control de acceso al soporte, MAC, recibir (72) por un nodo de conmutación de acceso, un paquete de autenticación enviado por un terminal de usuario que está conectado a una interfaz en el nodo de conmutación de acceso;

obtener (73), por el nodo de conmutación de acceso, un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido;

enviar (74), por el nodo de conmutación de acceso, la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido a un controlador por intermedio de un túnel de control establecido, de modo que el controlador mantenga una correspondencia entre la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido;

recibir (75), por el nodo de conmutación de acceso, el identificador de interfaz enviado por el controlador por intermedio del túnel de control, en donde el identificador de interfaz es un identificador de interfaz que se determina a partir de la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz después de que el controlador ponga en práctica, de forma satisfactoria, la autenticación de acceso en el terminal de usuario correspondiente a la dirección MAC, y está en correspondencia con la dirección MAC del terminal de usuario satisfactoriamente autenticado; y

activar, por el nodo de conmutación de acceso en conformidad con el identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz.

4. El método según la reivindicación 3, que comprende, además: recibir, por el nodo de conmutación de agregación, un permiso de acceso que es del terminal de usuario correspondiente a la dirección MAC y se envía por el controlador por intermedio del túnel de control; y

la activación por el nodo de conmutación de acceso, de conformidad con el identificador de interfaz recibido, de la interfaz correspondiente al identificador de interfaz comprende:

configurar o modificar, en conformidad con un permiso de acceso recibido enviado por el nodo de conmutación de agregación, el permiso de acceso de la interfaz que está en el nodo de conmutación de acceso y correspondiente al identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para acceder a una red en función del permiso de acceso.

5. El método según la reivindicación 3 o 4, en donde la obtención, por el nodo de conmutación de acceso, de un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y la obtención de una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido, comprende:

determinar, por el nodo de conmutación de acceso utilizando un procesador de señal que es capaz de realizar una función de procesamiento en conformidad con un código de programa, el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y transmitir el paquete de autenticación recibido al procesador de señal del nodo de conmutación de acceso; y obtener, por el procesador de señal a partir de un campo de dirección MAC origen del paquete de autenticación, la dirección MAC del terminal de usuario que envía el paquete de autenticación.

6. Un aparato para controlar el acceso de un terminal de usuario, que comprende:

un módulo de recepción (701), configurado para: recibir un paquete de autenticación enviado por intermedio de un túnel de datos establecido, y transmitir el paquete de autenticación recibido a un módulo de obtención;

el módulo de obtención (702) configurado para: obtener el paquete de autenticación transmitido por el módulo de recepción, obtener una dirección de control de acceso al soporte, MAC, en un campo de dirección MAC origen del paquete de autenticación, y transmitir la dirección MAC obtenida a un módulo de autenticación;

el módulo de autenticación (703), configurado para: recibir la dirección MAC transmitida por el módulo de obtención, poner en práctica la autenticación de acceso sobre un terminal de usuario correspondiente a la dirección MAC y transmitir un resultado de autenticación satisfactoria a un módulo de determinación;

el módulo de determinación (704), configurado para: obtener el resultado de la realización satisfactoria de la autenticación transmitido por el módulo de autenticación; determinar, a partir de una correspondencia mantenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, en donde el identificador de interfaz es un identificador de interfaz de un interfaz de un nodo de conmutación de acceso conectado al terminal de usuario; y transmitir el identificador de interfaz a un módulo de envío; y

el módulo de envío (705), configurado para: obtener el identificador de interfaz transmitido por el módulo de determinación, enviar el identificador de interfaz determinado al nodo de conmutación de acceso por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, y dar instrucciones al nodo de conmutación de acceso para activar la interfaz correspondiente a la identificador de interfaz.

7. El aparato según la reivindicación 6, en donde:

el módulo de recepción está configurado, además, para: recibir la dirección MAC del terminal de usuario enviada por el nodo de conmutación de acceso por intermedio del túnel de control, y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario, en donde la dirección MAC del terminal de usuario y el identificador de interfaz de la interfaz en el nodo de conmutación de acceso conectado al terminal de usuario se obtienen por el nodo de conmutación de acceso cuando el terminal de usuario establece una conexión con la interfaz en el nodo de conmutación de acceso, y envía un paquete por intermedio de la interfaz conectada, y transmitir la dirección MAC recibida y el identificador de interfaz recibido a un módulo de establecimiento; y

el aparato comprende, además, el módulo de establecimiento, configurado para: obtener la dirección MAC y el identificador de interfaz que se transmiten por el módulo de recepción, y establecer una correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz en conformidad con la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido.

8. Un aparato para controlar el acceso de un terminal de usuario, que comprende:

un módulo de recepción (901), configurado para: cuando se desactiva una función de aprendizaje de control de acceso al soporte, MAC, recibir un paquete de autenticación enviado por un terminal de usuario que está conectado a una interfaz en un nodo de conmutación de acceso, y transmitir el paquete de autenticación a un módulo de obtención;

el módulo de obtención (902), configurado para: recibir el paquete de autenticación transmitido por el módulo de recepción, obtener un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete

de autenticación, obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido y transmitir el identificador de interfaz y la dirección MAC a un módulo de envío;

el módulo de envío (903), configurado para: recibir el identificador de interfaz y la dirección MAC que se transmiten por el módulo de obtención, y enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz obtenido a un controlador por intermedio de un túnel de control establecido entre el controlador y el nodo de conmutación de acceso, de modo que el controlador mantenga una correspondencia entre la dirección MAC recibida del terminal de usuario y el identificador de interfaz recibido; en donde

el módulo de recepción (901) está configurado, además, para: recibir el identificador de interfaz enviado por el controlador por intermedio del túnel de control, y transmitir el identificador de interfaz a un módulo de control, en donde el identificador de interfaz es un identificador de interfaz que se determina a partir de la correspondencia entre la dirección MAC del terminal de usuario y el identificador de interfaz después de que el controlador realice, de forma satisfactoria, la autenticación de acceso en el terminal de usuario correspondiente a la dirección MAC, y está en correspondencia con la dirección MAC del terminal de usuario satisfactoriamente autenticado; y

el módulo de control (904) configurado para: obtener el identificador de interfaz transmitido por el módulo de recepción, y activar, en conformidad con el identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz.

9. El aparato según la reivindicación 8, en donde el módulo de recepción está configurado, además, para: recibir un permiso de acceso que es del terminal de usuario que es correspondiente a la dirección MAC y se envía por el controlador por intermedio del túnel de control, y transmitir el permiso de acceso al módulo de control; y

el módulo de control está específicamente configurado para: obtener el permiso de acceso transmitido por el módulo de recepción, y configurar o modificar, en conformidad con un permiso de acceso recibido enviado por un nodo de conmutación de agregación, el permiso de acceso de la interfaz que está en el nodo de conmutación de acceso y correspondiente al identificador de interfaz, para controlar el terminal de usuario, que está conectado a la interfaz, para tener acceso a una red de conformidad con el permiso de acceso.

10. El aparato según la reivindicación 8 o 9, en donde el módulo de obtención comprende específicamente un procesador de señal que es capaz de realizar una función de procesamiento en conformidad con un código de programa, y está configurado para: determinar el identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autenticación, y obtener el paquete de autenticación transmitido por el módulo de recepción; y el procesador de señal obtiene, a partir de un campo de dirección de MAC origen del paquete de autenticación, la dirección MAC del terminal de usuario que envía el paquete de autenticación.

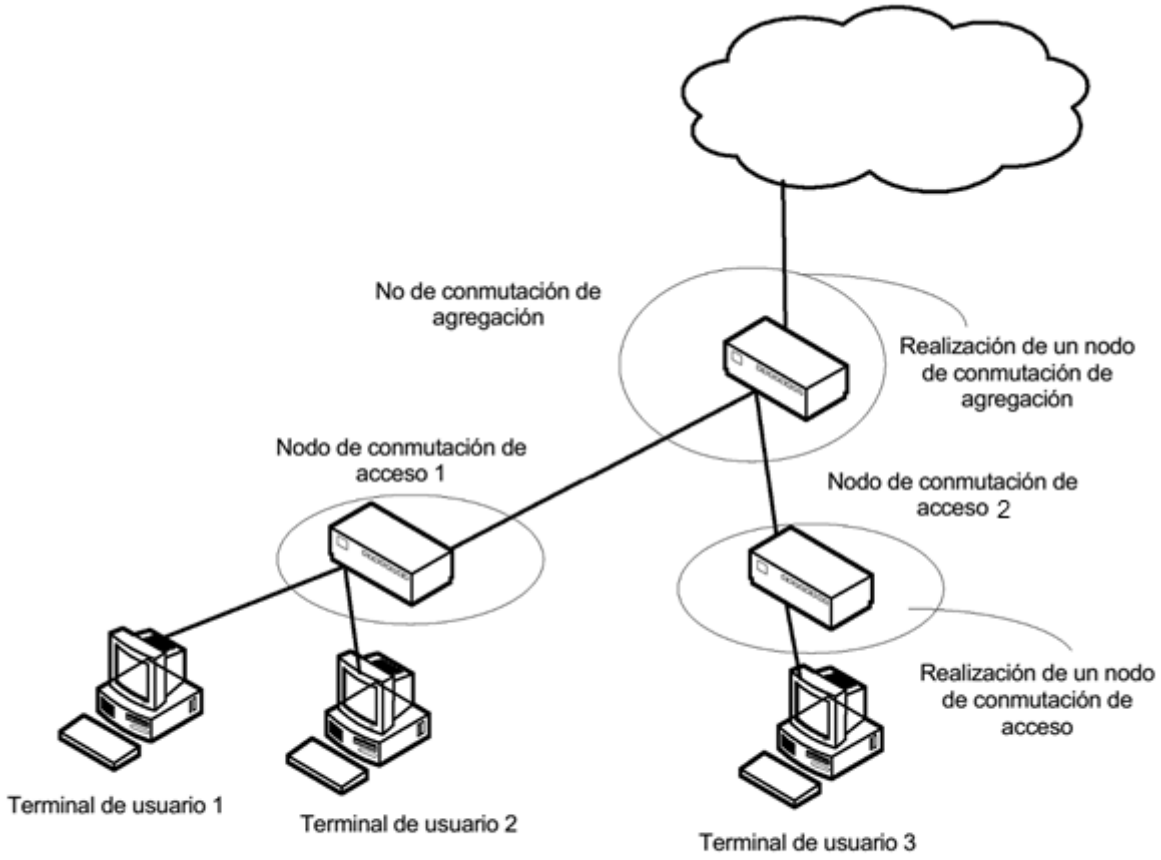
No de conmutación de agregación
Realización de un nodo de conmutación de agregación
Nodo de conmutación de acceso 1
Nodo de conmutación de acceso 2
Realización de un nodo de conmutación de acceso
Terminal de usuario 1
Terminal de usuario 2
Terminal de usuario 3

FIG. 1

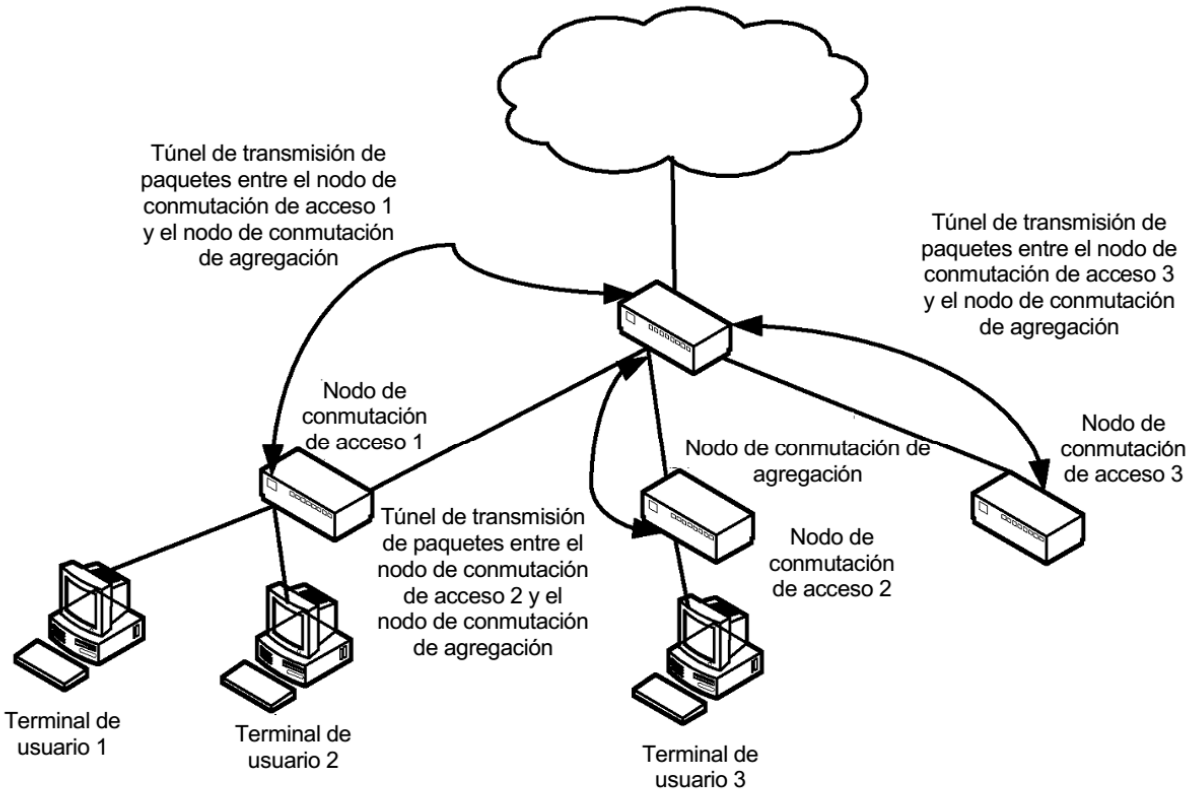
Túnel de transmisión de paquetes entre el nodo de conmutación de acceso 1 y el nodo de conmutación de agregación
Túnel de transmisión de paquetes entre el nodo de conmutación de acceso 3 y el nodo de conmutación de agregación
Nodo de conmutación de acceso 1
Nodo de conmutación de agregación
Nodo de conmutación de acceso 3
Túnel de transmisión de paquetes entre el nodo de conmutación de acceso 2 y el nodo de conmutación de agregación
Nodo de conmutación de acceso 2
Terminal de usuario 1
Terminal de usuario 2
Terminal de usuario 3

FIG. 2

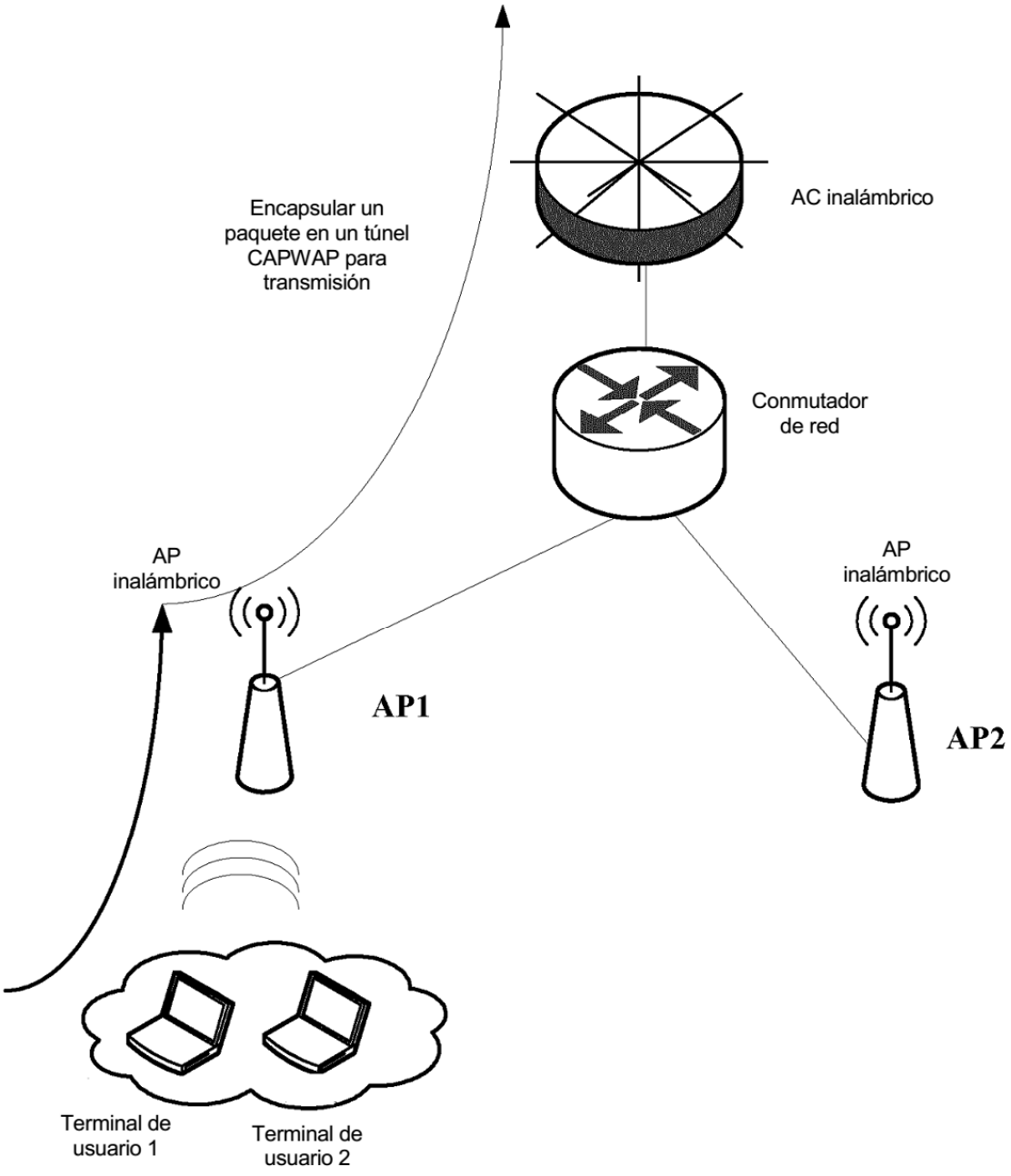
Encapsular un paquete en un túnel CAPWAP para transmisión
AC inalámbrico
Conmutador de red
AP inalámbrico
AP1
AP inalámbrico
AP2
Terminal de usuario 1
Terminal de usuario 2

FIG. 3a

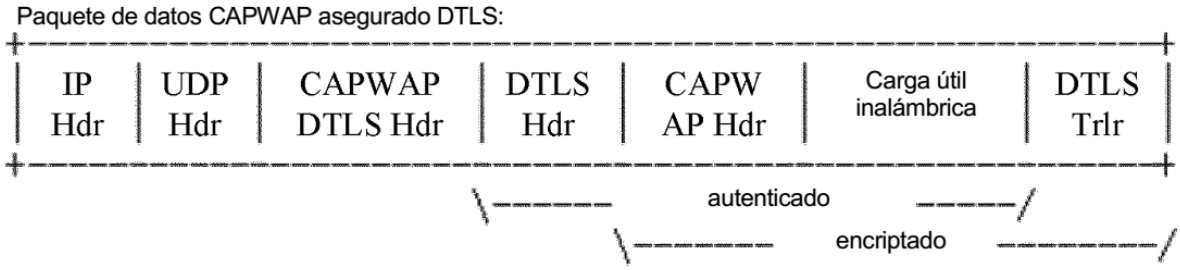

FIG. 3b

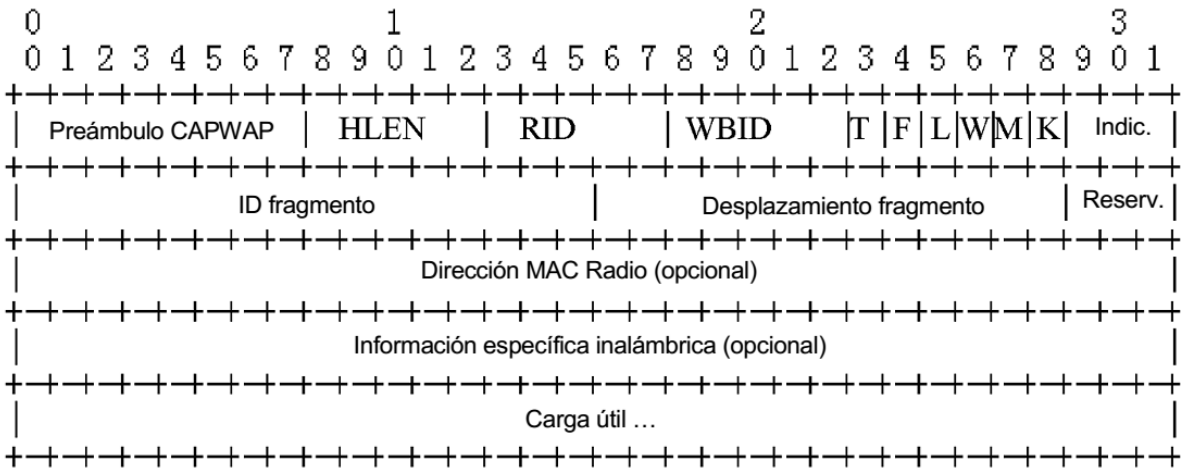

FIG. 3c

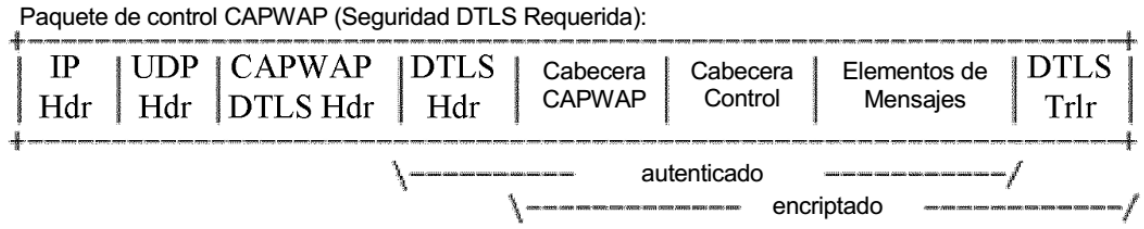

FIG. 3d

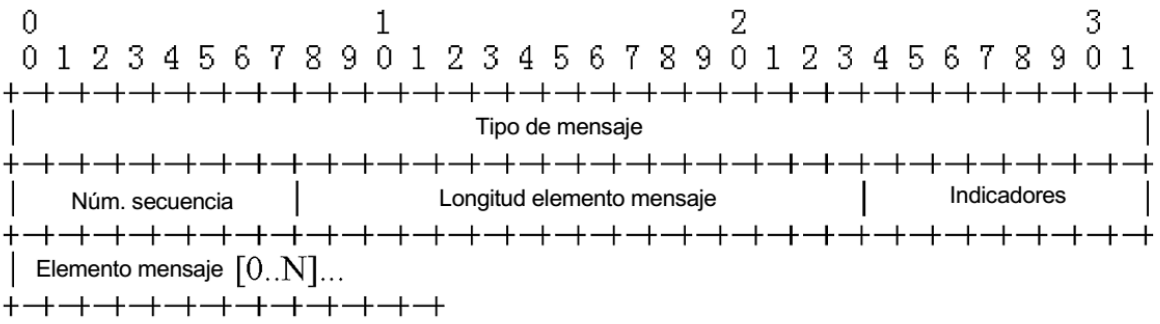
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo de mensaje
Núm. secuencia
Longitud elemento mensaje
Indicadores
Elemento mensaje [0..N]...

FIG. 3e

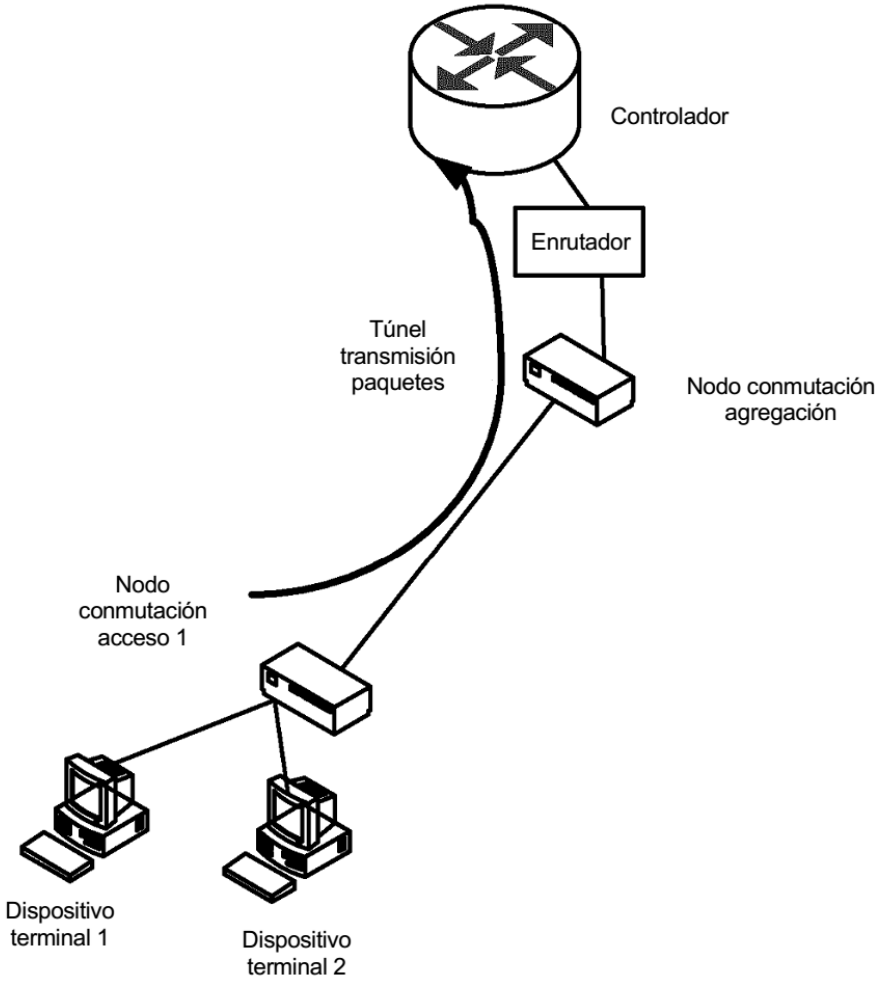
Controlador
Enrutador
Túnel transmisión paquetes
Nodo conmutación agregación
Nodo conmutación acceso 1
Dispositivo terminal 1
Dispositivo terminal 2

FIG. 4

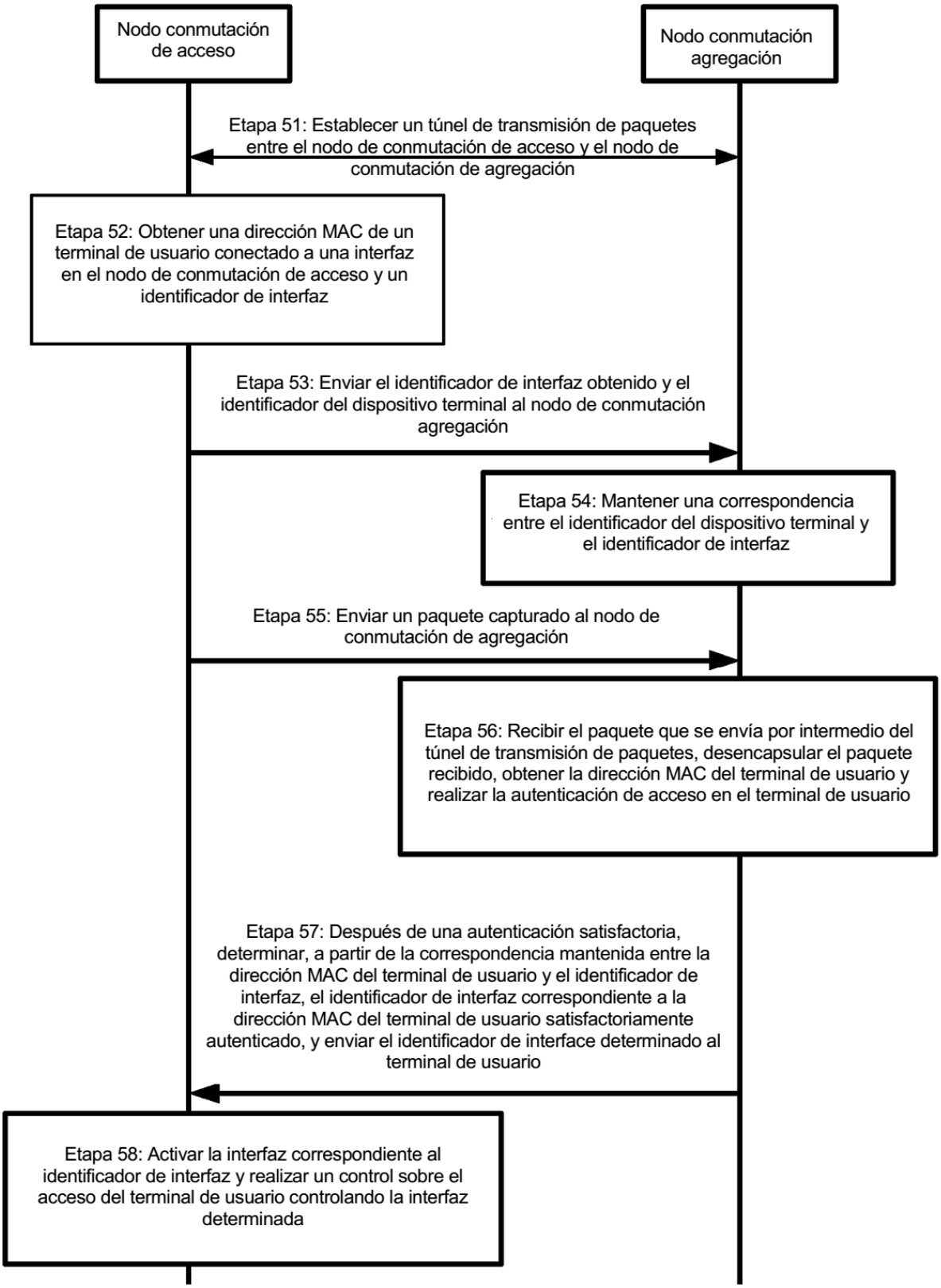
Nodo conmutación de acceso
Nodo conmutación agregación
Etapa 51: Establecer un túnel de transmisión de paquetes entre el nodo de conmutación de acceso y el nodo de conmutación de agregación
Etapa 52: Obtener una dirección MAC de un terminal de usuario conectado a una interfaz en el nodo de conmutación de acceso y un identificador de interfaz
Etapa 53: Enviar el identificador de interfaz obtenido y el identificador del dispositivo terminal al nodo de conmutación agregación
Etapa 54: Mantener una correspondencia entre el identificador del dispositivo terminal y el identificador de interfaz
Etapa 55: Enviar un paquete capturado al nodo de conmutación de agregación
Etapa 56: Recibir el paquete que se envía por intermedio del túnel de transmisión de paquetes, desencapsular el paquete recibido, obtener la dirección MAC del terminal de usuario y realizar la autenticación de acceso en el terminal de usuario
Etapa 57: Después de una autenticación satisfactoria, determinar, a partir de la correspondencia mantenida entre la dirección MAC del terminal de usuario y el identificador de interfaz, el identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado, y enviar el identificador de interface determinado al terminal de usuario
Etapa 58: Activar la interfaz correspondiente al identificador de interfaz y realizar un control sobre el acceso del terminal de usuario controlando la interfaz determinada

FIG. 5

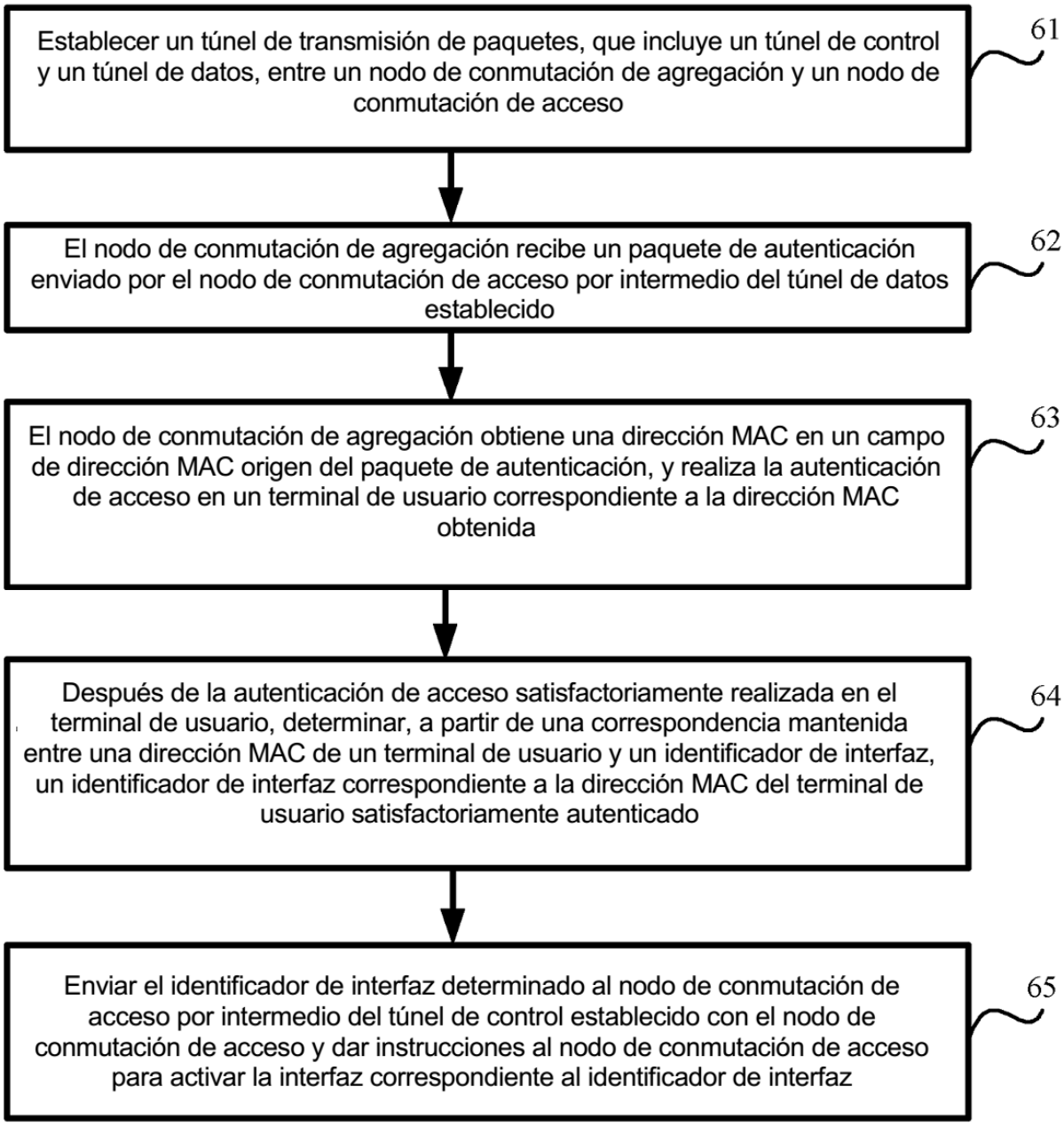
Establecer un túnel de transmisión de paquetes, que incluye un túnel de control y un túnel de datos, entre un nodo de conmutación de agregación y un nodo de conmutación de acceso
61
El nodo de conmutación de agregación recibe un paquete de autenticación enviado por el nodo de conmutación de acceso por intermedio del túnel de datos establecido
62
El nodo de conmutación de agregación obtiene una dirección MAC en un campo de dirección MAC origen del paquete de autenticación, y realiza la autenticación de acceso en un terminal de usuario correspondiente a la dirección MAC obtenida
63
Después de la autenticación de acceso satisfactoriamente realizada en el terminal de usuario, determinar, a partir de una correspondencia mantenida entre una dirección MAC de un terminal de usuario y un identificador de interfaz, un identificador de interfaz correspondiente a la dirección MAC del terminal de usuario satisfactoriamente autenticado
64
Enviar el identificador de interfaz determinado al nodo de conmutación de acceso por intermedio del túnel de control establecido con el nodo de conmutación de acceso y dar instrucciones al nodo de conmutación de acceso para activar la interfaz correspondiente al identificador de interfaz
65

FIG. 6a

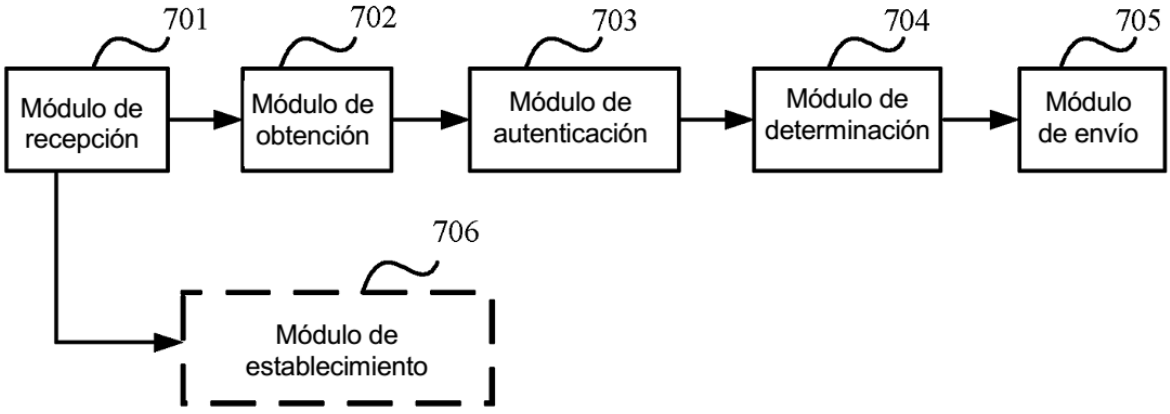
701
Módulo de recepción
702
Módulo de obtención
703
Módulo de autenticación
704
Módulo de determinación
705
Módulo de envío
706
Módulo de establecimiento

FIG. 6b

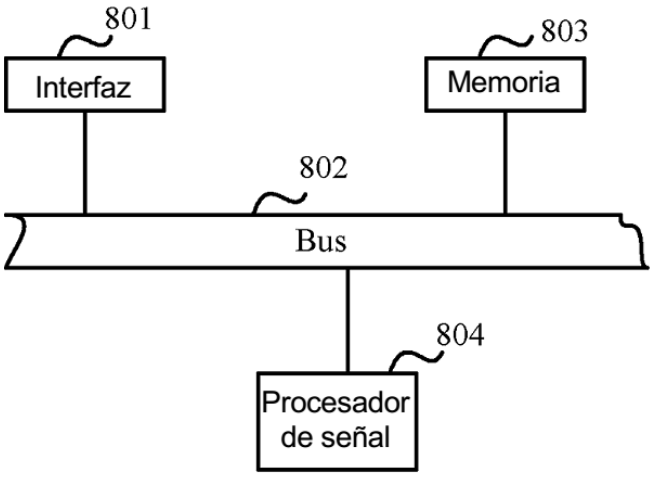
801
Interfaz
803
Memoria
802
Bus
804
Procesador de señal

FIG. 6c

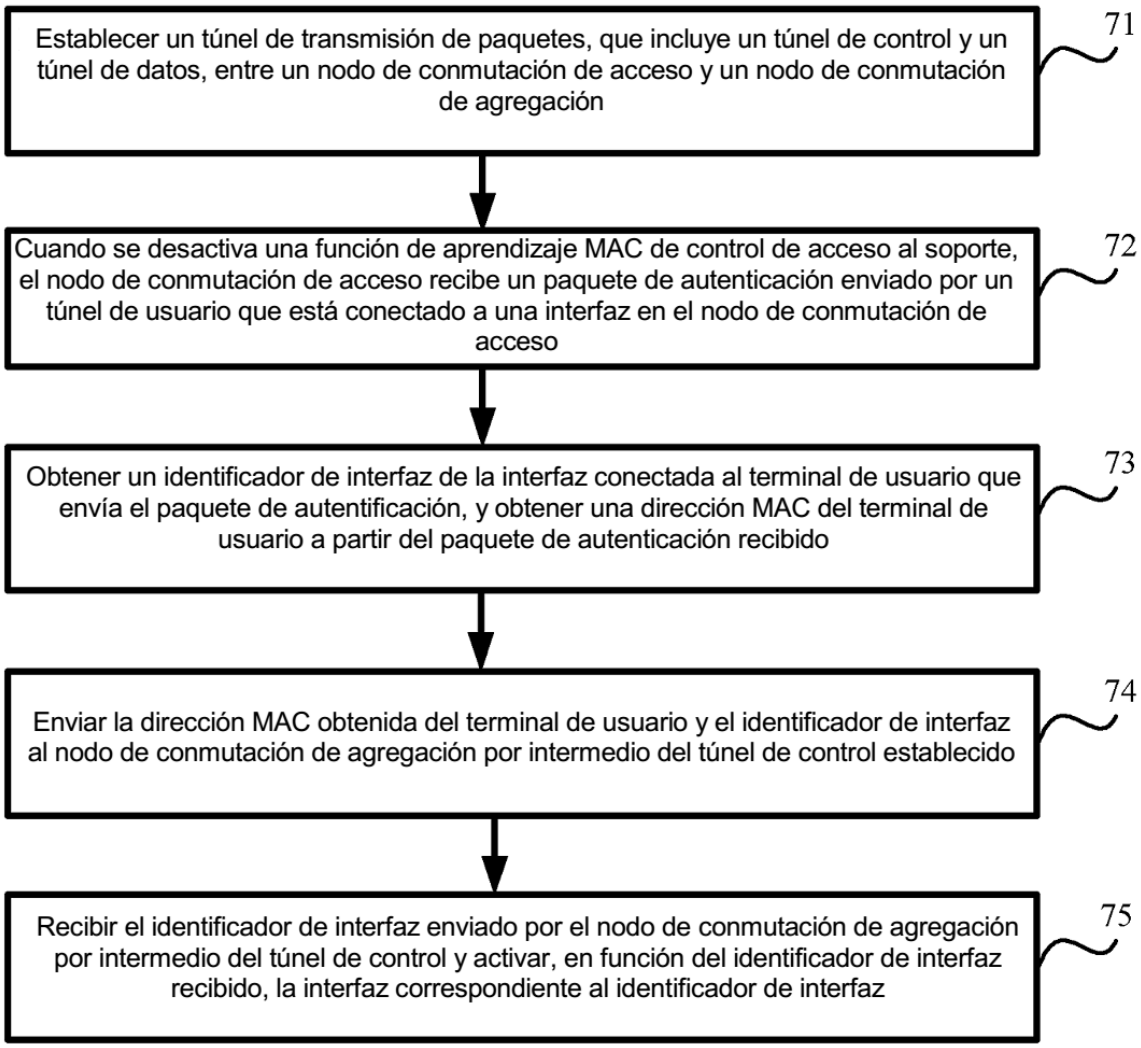
Establecer un túnel de transmisión de paquetes, que incluye un túnel de control y un túnel de datos, entre un nodo de conmutación de acceso y un nodo de conmutación de agregación
71
Cuando se desactiva una función de aprendizaje MAC de control de acceso al soporte, el nodo de conmutación de acceso recibe un paquete de autenticación enviado por un túnel de usuario que está conectado a una interfaz en el nodo de conmutación de acceso
72
Obtener un identificador de interfaz de la interfaz conectada al terminal de usuario que envía el paquete de autentificación, y obtener una dirección MAC del terminal de usuario a partir del paquete de autenticación recibido
73
Enviar la dirección MAC obtenida del terminal de usuario y el identificador de interfaz al nodo de conmutación de agregación por intermedio del túnel de control establecido
74
Recibir el identificador de interfaz enviado por el nodo de conmutación de agregación por intermedio del túnel de control y activar, en función del identificador de interfaz recibido, la interfaz correspondiente al identificador de interfaz
75

FIG. 7a

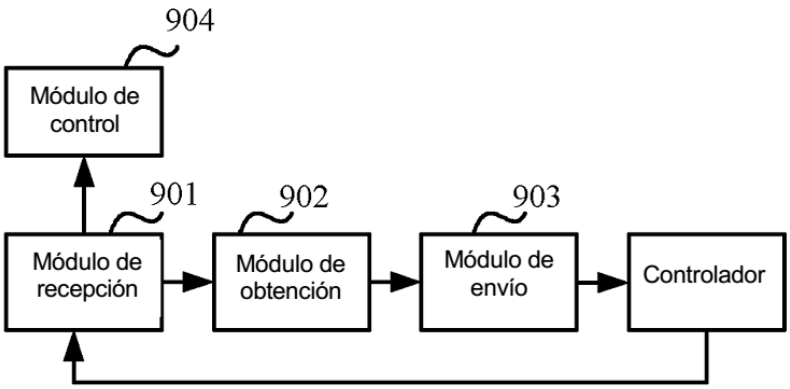
904
Módulo de control
901
902
903
Módulo de recepción
Módulo de obtención
Módulo de envío
Controlador

FIG. 7b

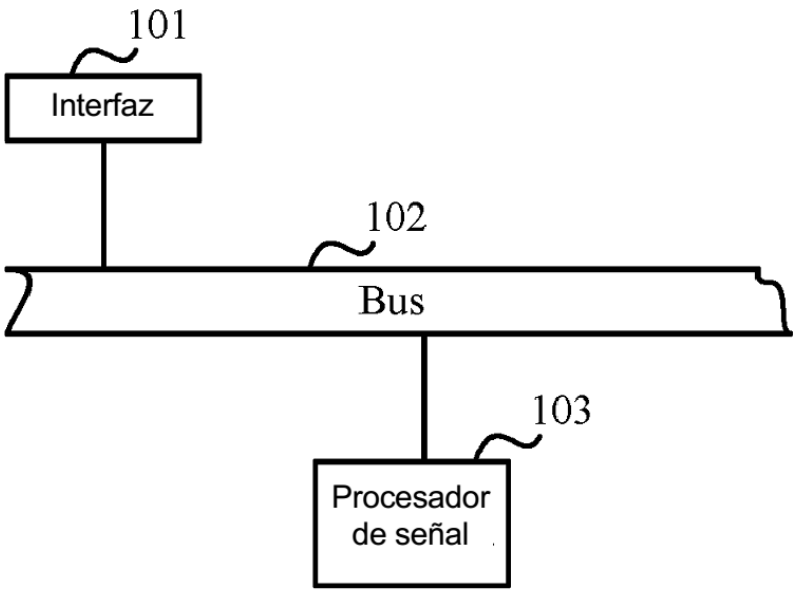

FIG. 7c