

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 960 879**

51 Int. Cl.:

H04L 41/5041	(2012.01) H04L 65/75	(2012.01)
H04L 41/12	(2012.01) H04L 41/5054	(2012.01)
H04L 45/64	(2012.01) H04W 12/00	(2011.01)
H04L 45/00	(2012.01) H04L 65/612	(2012.01)
H04L 45/745	(2012.01)	
H04L 49/35	(2012.01)	
H04L 9/40	(2012.01)	
H04L 41/40	(2012.01)	
H04L 65/65	(2012.01)	
H04L 65/70	(2012.01)	

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **07.01.2019** **PCT/US2019/012467**

87 Fecha y número de publicación internacional: **18.07.2019** **WO19139840**

96 Fecha de presentación y número de la solicitud europea: **07.01.2019** **E 19738202 (1)**

97 Fecha y número de publicación de la concesión europea: **23.08.2023** **EP 3738276**

54 Título: **Aislamiento de servicios a través de una única interfaz física de red**

30 Prioridad:

09.01.2018 US 201815866336

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
07.03.2024

73 Titular/es:

ENTRYPOINT NETWORKS, INC. (100.0%)
1949 West Printers Row
Salt Lake City UT 84119, US

72 Inventor/es:

PETERSON, JEFFREY;
TURNER, ERIC y
PETERSON, ROBERT

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 960 879 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Aislamiento de servicios a través de una única interfaz física de red

Campo de la invención

Esta invención se refiere a un método llevado a cabo por un dispositivo de red, a un medio de almacenamiento informático y a un sistema de red definido por software.

Antecedentes

Redes definidas por software (SDN, por sus siglas en inglés) es un término general que incluye una serie de tecnologías de red. SDN tiene como objetivo separar el plano de control de la red del plano de datos de la red para crear una red ágil y flexible. En una red definida por software, el conmutador o conmutadores u otros componentes que forman la topología física de la red pueden comunicarse con el controlador para determinar cómo se deben dirigir las tramas (frames) dentro de la red. De esta manera, el controlador puede crear, modificar o eliminar conexiones entre dos puntos finales para suministrar servicios dinámicamente entre los puntos finales.

Durante este suministro de servicios, es importante tener en cuenta que la topología física de la red permanece sin cambios. En vez de eso, para proporcionar un servicio entre dos puntos finales (p. ej., entre el hogar de un usuario y un conmutador de borde de un proveedor), el controlador normalmente empleará conocimiento de la topología de la red, incluyendo cómo los puntos finales están físicamente interconectados, el tráfico actual en la red y cualquier requisito de calidad del servicio (entre otros posibles factores) para seleccionar y crear una red virtual entre los puntos finales. Esto se logra programando los conmutadores apropiados u otros componentes para reenviar tramas pertenecientes al servicio de modo que atraviesen una ruta seleccionada para llegar a su punto final. En algunas implementaciones, sólo los componentes ubicados en el borde de la topología de la red pueden implementar esta técnica de red definida por software.

Existen varios protocolos y técnicas para proporcionar servicios de esta manera. Por ejemplo, una red definida por software puede configurarse para emplear etiquetas VLAN (u otros identificadores) dentro de las tramas para definir a qué servicio pertenecen las tramas. Accediendo a la etiqueta VLAN en una trama que reciba, un conmutador puede determinar, basándose en sus reglas programadas, cómo reenviar la trama para que la trama atravesase la ruta que fue definida para ese servicio. En este tipo de entorno, las tramas pertenecientes a múltiples servicios se pueden transferir a través del mismo cable físico pero permanecen aisladas debido a las etiquetas VLAN que incluyen.

La Figura 1 proporciona un ejemplo simplificado de una arquitectura 100 de red definida por software de la técnica anterior. La arquitectura 100 incluye una red 130 que consta de varios conmutadores interconectados 130a-130n que forman una estructura de conmutación (donde n representa cualquier número entero mayor que uno). Varias entidades pueden conectarse a la red 130, incluidos proveedores de servicios y usuarios finales. Los proveedores de servicios normalmente pueden incluir una red que se conecta a la red 130 a través de un conmutador de borde. Por el contrario, un usuario final normalmente puede emplear una puerta de enlace para conectarse a la red 130. Un controlador 131 puede controlar componentes dentro de la arquitectura 100. En algunas realizaciones, el controlador 131 puede configurar la puerta 110 de enlace con el fin de suministrar servicios entre el usuario final y un proveedor de servicios. En algunas realizaciones, el controlador 131 también puede configurar el conmutador 132 de borde o algunos o todos los conmutadores 130a-130n para suministrar dichos servicios.

En un ejemplo, una red 140a de un proveedor de vídeo en *streaming* (p. ej., Netflix, Hulu, Sling, etc.), una red 140b de un proveedor de servicios de Internet y una red 140n de un proveedor de seguridad se pueden conectar cada una a un puerto particular del conmutador 132 de borde. Además, las instalaciones de un usuario (p. ej., un hogar o un local comercial) incluyen una *smart TV* 100a, un PC 100b y un sistema 100n de seguridad.

El usuario puede desear emplear la *smart TV* 100a, el PC 100b y el sistema 100n de seguridad para que reciban servicios a través de la red 130. Para conectar la *smart TV* 100a, el PC 100b y el sistema 100n de seguridad (o cualquier otro dispositivo conectable a red) a la red 130, el usuario puede emplear la puerta 110 de enlace. La puerta 110 de enlace incluye un puerto 112 de salida (o de red de área amplia (WAN, por sus siglas en inglés)) mediante el cual se conecta a un conmutador (p. ej., el conmutador 130c) de la red 130. La puerta 110 de enlace también incluye una serie de puertos 111a-111n de entrada (o de red de área local (LAN, por sus siglas en inglés)) mediante los cuales el usuario final puede conectar los diversos dispositivos a la puerta 110 de enlace.

Una distinción importante entre una red definida por software y una conexión a Internet típica es que una red definida por software permite al usuario acceder a un servicio independientemente de Internet. Por ejemplo, en un escenario basado en Internet, si el usuario desea suscribirse a Netflix, primero debe suscribirse a un proveedor de servicios de Internet (p. ej., Comcast, Verizon, Time Warner, AT&T, etc.) para acceder a Netflix. En este escenario, el usuario accede a Netflix a través de Internet. Por el contrario, con una red definida por software y asumiendo que la red proveedora 140a de vídeo en *streaming* es Netflix, el controlador 131 puede suministrar la entrega de Netflix a las instalaciones del usuario independientemente de cualquier acceso a Internet.

Como se mencionó anteriormente, la arquitectura 100 puede usar identificadores de capa dos (en lo sucesivo

generalmente "ID") para distinguir entre diferentes servicios que se han suministrado a través de la red 130. Por ejemplo, a un servicio de vídeo en *streaming* que se ha suministrado para el usuario final se le podría asignar un ID de 1234. En tal caso, cualquier trama que el proveedor de vídeo en *streaming* envíe al usuario final se etiquetará con 1234. En el lado del servicio, este etiquetado de tramas se lleva a cabo en el conmutador de borde mediante el cual la red del proveedor está conectada a la red 130. Por lo tanto, el conmutador 132 de borde etiquetaría una trama que estuviera destinada al usuario final con 1234 si esa trama se recibiera a través del puerto asociado con la red 140a del proveedor de vídeo en *streaming*.

Como se mencionó anteriormente, la puerta 110 de enlace incluye múltiples puertos 111a-111n de entrada. Esto es necesario para permitir que se entreguen múltiples servicios a las instalaciones del usuario a través de la puerta 110 de enlace. En particular, como parte del suministro de un servicio a las instalaciones del usuario, el controlador 131 puede ordenar a la puerta 110 de enlace que entregue tramas entrantes que tengan un ID particular a uno de los puertos 111a-111n. De manera similar, el controlador 131 puede ordenar a la puerta 110 de enlace que asigne el ID particular a cualquier trama saliente que se reciba en el mismo puerto. En otras palabras, cada servicio entregado en las instalaciones del usuario requiere su propio puerto de entrada en la puerta 110 de enlace.

Por consiguiente, en la Figura 1, se asume que el servicio de vídeo en *streaming* se proporciona a las instalaciones del usuario a través del puerto 111a, el servicio de Internet se proporciona a través del puerto 111b y el servicio del sistema de seguridad se proporciona a través del puerto 111n. En este escenario, la puerta 110 de enlace crea la apariencia de que hay múltiples redes separadas disponibles en las instalaciones del usuario (es decir, la puerta 110 de enlace proporciona múltiples redes virtuales).

Aunque esta relación uno a uno entre servicios y puertos proporciona aislamiento de servicios, también crea varias dificultades prácticas. Por ejemplo, para utilizar un servicio en un dispositivo, el dispositivo deberá estar conectado al puerto apropiado. En la Figura 1, la *smart TV* 100a deberá estar conectada (ya sea mediante un cable Ethernet, Wi-Fi u otra interfaz) al puerto 111a para poder utilizar el servicio vídeo en *streaming*. Por otro lado, el PC 100b deberá estar conectado al puerto 111b para utilizar Internet. En este escenario, Internet no estará disponible en la *smart TV* 100a y el servicio de vídeo en *streaming* no estará disponible en el PC 100b. También puede resultar difícil conectar físicamente cada dispositivo al puerto adecuado. Por ejemplo, muchos hogares y negocios están cableados para una única red que es compartida por todos los dispositivos. En tales casos, sería necesario comprar múltiples routers para emplear redes Wi-Fi separadas para cada servicio y/o agregar cableado adicional para conectar los dispositivos al puerto apropiado de la puerta 110 de enlace. Además, en muchos casos, la puerta 110 de enlace puede no estar ubicada dentro del edificio o en un área fácilmente accesible.

La patente europea EP 3 066 802 A1 describe un sistema y método para dirigir el tráfico a través de un conjunto de servicios. Se asigna una ruta de servicios o cadena de servicios a un paquete recibido basándose en una clasificación del paquete y correlación del paquete con un flujo de tráfico. Se puede crear un nuevo identificador de cadena de servicios si no existe dicha correlación. Se pueden determinar un tipo de servicio siguiente y una instancia particular del tipo de servicio siguiente de acuerdo con el identificador de cadena de servicios. Se puede establecer un destino siguiente para el tráfico de acuerdo con la instancia del servicio siguiente.

La patente US 2016/352538 A1 describe una inserción de servicio de red que incluye determinar una interfaz de túnel correspondiente a una entidad de servicio a la que se va a dirigir un paquete entrante, determinándose la interfaz de túnel basándose en reglas de flujo de red definida por software (SDN). Además, el paquete entrante se puede encapsular basándose en una configuración de túnel correspondiente a la interfaz de túnel para generar un paquete encapsulado de modo que el paquete encapsulado incluya encabezados de dirección de control de acceso al medio (MAC, por sus siglas en inglés) y una etiqueta de red de área local virtual (VLAN, por sus siglas en inglés) asociada con el paquete entrante. El paquete encapsulado se puede enviar a la entidad de servicio a través de la interfaz de túnel para la inserción del servicio de red.

Compendio

Las realizaciones de la presente invención se extienden a métodos, sistemas y productos de programas de ordenador para aislar servicios a través de una única interfaz física de red. Una puerta de enlace que está instalada en las instalaciones del usuario puede incluir un único puerto de entrada a través del cual se pueden proporcionar múltiples servicios a las instalaciones. La puerta de enlace puede evaluar todas las tramas salientes que se reciben en el puerto para identificar a qué servicio pertenecen y luego etiquetar las tramas con un identificador asignado al servicio. Este etiquetado permitirá que las tramas se entreguen al proveedor de servicios previsto. Cuando la puerta de enlace recibe una trama entrante, puede retirar el identificador de la trama y reenviarla a través del único puerto entrante independientemente del servicio al que pertenece. De esta manera, múltiples servicios que se proporcionan a las instalaciones del usuario pueden permanecer aislados en la red de área amplia incluso aunque se proporcionen a través del mismo medio físico en la red de área local del usuario.

Según un aspecto, se proporciona un método según la reivindicación 1.

Según otro aspecto, se proporcionan uno o más medios de almacenamiento informático según la reivindicación 11.

Según otro aspecto, se proporciona una arquitectura de red definida por software según la reivindicación 18.

En las reivindicaciones dependientes se definen otras características según realizaciones.

Este compendio se proporciona para presentar de una forma simplificada una selección de conceptos, que se describen con más detalle a continuación en la Descripción detallada. Este Compendio no pretende identificar características clave o características esenciales de la materia objeto reivindicada.

- 5 La invención está definida por las reivindicaciones adjuntas.

Breve descripción de los dibujos

- 10 Para describir la manera en que se pueden obtener las ventajas y características mencionadas anteriormente, y otras, de la invención, se realizará una descripción más particular de la invención descrita brevemente anteriormente haciendo referencia a realizaciones específicas de la misma que se ilustran en los dibujos adjuntos. Entendiendo que estos dibujos representan sólo realizaciones típicas de la invención y, por lo tanto, no deben considerarse limitativos de su alcance, la invención se describirá y explicará con especificidad y detalle adicionales mediante el uso de los dibujos adjuntos en los que:

La Figura 1 ilustra un ejemplo de una arquitectura de red definida por software de la técnica anterior;

- 15 La Figura 2 ilustra una arquitectura de red definida por software de acuerdo con realizaciones de la presente invención;

Las Figuras 3A-3D ilustran un proceso mediante el cual las tramas recibidas a través de un puerto común pueden modificarse para que incluyan un identificador específico del servicio;

La Figura 4 también ilustra cómo se pueden modificar las tramas recibidas a través de un puerto común para que incluyan un identificador específico del servicio; y

- 20 La Figura 5 proporciona un diagrama de flujo de un método de ejemplo para modificar tramas para que incluyan un identificador específico del servicio.

Descripción detallada

- En esta especificación y las reivindicaciones, una puerta de enlace debe interpretarse como un dispositivo electrónico que incluye al menos un puerto de salida para acoplarse a una WAN y al menos un puerto de entrada para acoplarse a una LAN. El término "capa dos" debe interpretarse como la capa de enlace de datos del modelo OSI, mientras que el término "capa tres" debe interpretarse como la capa de red del modelo OSI. Un identificador (o ID) de capa dos debe abarcar cualquiera de los diversos tipos de identificadores que pueden añadirse a una trama, incluidos, por ejemplo, una etiqueta VLAN, una etiqueta MPLS o una etiqueta de segmento de enrutamiento de segmentos (*Segment Routing*). La presente invención no debe limitarse a ningún protocolo de capa dos particular. Sólo con fines ilustrativos, podrían usarse el protocolo 802.1Q o el 802.1ad en realizaciones de la presente invención. El término "puerto" debe interpretarse como una interfaz física de capa dos y no debe confundirse con puertos lógicos en la capa de transporte.

- 35 La Figura 2 ilustra un ejemplo de arquitectura 200 de red definida por software que está configurada de acuerdo con realizaciones de la presente invención. Para simplificar la descripción, la arquitectura 200 incluye la misma configuración de la red 130 y las redes 140a-140n de proveedores como se muestra en la Figura 1. Esto también pretende representar que la presente invención se puede implementar en redes existentes.

- En contraste con la Figura 1, la arquitectura 200 incluye una puerta 210 de enlace que tiene un puerto 212 de salida y un único puerto 211 de entrada. Se observa que la puerta 210 de enlace podría tener múltiples puertos de entrada, pero las técnicas de la presente invención pertenecen a la gestión de tramas a través de un único puerto de entrada. Por lo tanto, las técnicas de la presente invención podrían implementarse independientemente en cada puerto de entrada de una puerta de enlace. También a diferencia de la Figura 1, la *smart TV* 100a, el PC 100b y el sistema 100n de seguridad están todos conectados al puerto 211 de entrada de la puerta 210 de enlace (p. ej., a través de un concentrador (*hub*) o un *rúter* 220). En consecuencia, en la presente invención, existe una relación de uno a muchos entre un puerto y los servicios proporcionados en las instalaciones del usuario.

- 45 Las Figuras 3A-3D ilustran cómo se puede implementar esta relación de uno a muchos dentro de la arquitectura 200 de ejemplo. En la Figura 3A, se asume que el usuario se ha suscrito a servicios de vídeo en *streaming* disponibles a través de la red 140a del proveedor de vídeo en *streaming*. La forma en que el usuario se suscribe no es esencial para la invención. Es importante el hecho de que el controlador 231 recibirá y/o accederá a información sobre la puerta 210 de enlace mediante la cual el usuario accede a la red 130 e información sobre el conmutador 132 de borde mediante el cual el proveedor de vídeo en *streaming* se conecta a la red 130. Con esta información, y en la etapa 1, el controlador 231 puede determinar cómo configurar la puerta 210 de enlace para suministrar una red virtual entre el usuario y el proveedor de vídeo en *streaming*. Esto puede incluir seleccionar un ID para añadirlo a las tramas enviadas entre el usuario y el proveedor de vídeo en *streaming* y definir criterios de coincidencia para ser usados por la puerta 210 de enlace para identificar qué tramas deben modificarse para que incluyan el ID seleccionado. Basándose en estas determinaciones, en la etapa 2, el controlador 231 puede enviar configuraciones a la puerta 210 de enlace para hacer

que modifique apropiadamente las tramas salientes. En este ejemplo, se asumirá que la dirección MAC de la *smart TV* 100a es MAC1 y la dirección IP donde están disponibles los servicios de vídeo en *streaming* es IP1.

Volviendo ahora a la Figura 3B, se asumirá que las configuraciones enviadas a la puerta 210 de enlace incluían un ID de ID1 y los criterios de coincidencia correspondientes que identifican una dirección MAC de origen de MAC1 y una dirección IP de destino de IP1. Por lo tanto, la etapa 3 representa que la puerta 210 de enlace ha creado o actualizado una tabla 300 de ID que incluye una primera entrada perteneciente al servicio de vídeo en *streaming* que asocia ID1 con MAC1 e IP1. Con fines ilustrativos, también se asumirá que la tabla 300 de ID ya incluye una entrada que asocia ID2 con MAC2 e IP2 y que esta segunda entrada pertenece a servicios de seguridad. El papel de la tabla 300 de ID es definir qué ID debe añadir la puerta 210 de enlace a las tramas salientes que recibe en el puerto 211. En consecuencia, después de la etapa 3, se habrá definido una red virtual entre la puerta 210 de enlace y el conmutador 132 de borde para permitir que las tramas fluyan entre el dispositivo del usuario (que se asume que es una *smart TV* 100a) y la red 140a del proveedor de vídeo en *streaming*.

Con la red virtual implementada, el usuario puede comenzar a recibir servicios de vídeo en *streaming* en la *smart TV* 100a (u otro dispositivo conectado a la puerta 210 de enlace, asumiendo que se han creado las entradas correspondientes en la tabla 300 de ID). Por ejemplo, en la Figura 3C, se asume que el usuario emplea la *smart TV* 100a para acceder al servicio de vídeo en *streaming*. Sólo como ejemplo, el usuario puede iniciar la aplicación Netflix en la *smart TV* 100a. Sin embargo, puede resultar el mismo proceso si el usuario empleó el PC 100b para acceder a Netflix (de nuevo asumiendo que se han creado las entradas correspondientes en la tabla 300 de ID). De acuerdo con los protocolos estándar, en la etapa 4, la *smart TV* 100a puede generar una trama que incluye la dirección IP del servicio de vídeo en *streaming* (IP1) como dirección de destino en el paquete IP y su propia dirección MAC (MAC1) como dirección de origen en la trama. Por supuesto, la trama también incluiría una dirección IP de origen (que probablemente será una dirección IP privada asignada a la *smart TV* 100a) y una dirección MAC de destino (que probablemente será la dirección MAC de la puerta 210 de enlace), entre otras cosas, pero estos campos se ignorarán en el ejemplo actual.

De manera importante, la puerta 210 de enlace recibirá esta trama a través del puerto 211, el mismo puerto por el cual la puerta 210 de enlace recibiría tramas pertenecientes a otros servicios a los que el usuario se ha suscrito (p. ej., comunicaciones de Internet, comunicaciones de seguridad, etc.). Para dirigir tramas a la red del proveedor prevista, la puerta 210 de enlace puede modificar las tramas salientes que recibe para que incluyan el ID adecuado. Esto se logra usando la tabla 300 de ID. Por ejemplo, en la etapa 5 y en respuesta a recibir la trama de la *smart TV* 100a en la etapa 4, la puerta 210 de enlace puede evaluar la trama y comparar su contenido con los criterios de coincidencia asociados con cada ID. En este caso, la puerta 210 de enlace determinará que la trama tiene una dirección MAC de origen de MAC1 y una dirección IP de destino de IP1. Con esta información, la puerta 210 de enlace puede buscar en la tabla 300 de ID para determinar que existe una coincidencia y que ID1 está asociado con estos criterios. Como resultado, la puerta 210 de enlace añadirá ID1 a la trama.

Se pueden añadir ID a las tramas de acuerdo con varios protocolos diferentes. Por ejemplo, los ID pueden estar en forma de etiqueta VLAN de acuerdo con los protocolos 802.1Q u 802.1ad, en forma de etiqueta de acuerdo con el protocolo MPLS, o en cualquier otro formato. Una vez que la puerta 210 de enlace ha añadido el ID adecuado, puede reenviar la trama modificada a través de la red 130 a través del puerto 212 como se representa en la etapa 6.

Cabe señalar que, en algunos casos, la puerta 210 de enlace puede modificar una trama para incluir un ID por defecto cuando la trama no coincide con ningún criterio en la tabla 300. Por lo tanto, siempre que la puerta 210 de enlace o cualquier otra puerta de enlace en la red reciba una trama que no coincide con ningún criterio, la trama puede modificarse para incluir el ID por defecto y luego reenviarse a través de la red. En resumen, la puerta 210 de enlace modifica selectivamente las tramas basándose en si el contenido de la trama coincide con una entrada o no coincide con ninguna entrada en la tabla 300 de ID.

Una vez que la puerta 210 de enlace reenvía la trama con el ID añadido de ID1 a través de la red 130, la trama se reenviará hacia el conmutador 132 de borde. En la etapa 7, el conmutador 132 de borde recibirá la trama y puede emplear el ID para determinar cómo reenviar la trama. En particular, el conmutador 132 de borde mantendrá una tabla que asocia uno o más ID con cada uno de sus puertos de entrada. En este ejemplo, ID1 se asociará con el puerto de entrada mediante el cual la red 140a del proveedor de vídeo en *streaming* está conectada al conmutador 132 de borde. Por lo tanto, el conmutador 132 de borde reenviará la trama a la red 140a del proveedor de vídeo en *streaming*.

En algunas realizaciones no reivindicadas, el conmutador 132 de borde puede retirar el ID de la trama antes de reenviarla a través de un puerto de entrada. Al eliminar el ID en el conmutador 132 de borde, no será necesario configurar los componentes de la red 140a del proveedor de vídeo en *streaming* para procesar dichos ID. En otras palabras, el uso de los ID es transparente para los componentes de la red del proveedor así como para los dispositivos del usuario.

Para ilustrar mejor cómo la presente invención aísla los servicios que se proporcionan a través del mismo puerto, la Figura 4 proporciona un ejemplo donde el sistema 100n de seguridad envía una trama dirigida a la red 140n del proveedor de seguridad. En este ejemplo, se asume que el sistema 100n de seguridad tiene una dirección MAC de MAC2 y que el proveedor de servicios de seguridad emplea una dirección IP de IP2 para los servicios de seguridad.

Por consiguiente, en la etapa 1 de la Figura 4, la puerta 210 de enlace recibe una trama del sistema 100n de seguridad a través del puerto 211, y esta trama incluye MAC2 como dirección MAC de origen e IP2 como dirección IP de destino. En la etapa 2, la puerta 210 de enlace consulta la tabla 300 de ID en busca de una entrada que coincida con el contenido de esta trama. En este caso, la puerta 210 de enlace determinará que ID2 se ha asociado con la dirección MAC de origen de MAC2 y la dirección IP de destino de IP2. En respuesta, la puerta 210 de enlace modificará la trama para que incluya ID2 y luego reenviará la trama modificada por el puerto 212 en la etapa 3. Por consiguiente, la puerta 210 de enlace permite que el servicio de vídeo en *streaming* y el servicio de seguridad se suministren a las instalaciones del usuario a través del mismo puerto 211 al mismo tiempo que se garantiza que estos servicios permanecen aislados.

En compendio, la puerta 210 de enlace puede mantener una tabla (o alguna otra estructura de datos) de ID que asocie cualquier combinación de criterios con un ID particular. La combinación de criterios puede incluir información de capa dos, información de capa tres o cualquier otra información que pueda extraerse de una trama que la puerta 210 de enlace recibe de un dispositivo del usuario y que identifique un servicio particular al que se dirige la trama. Evaluando las tramas, la puerta 210 de enlace puede añadir el ID apropiado a cada trama para hacer que la trama se entregue al proveedor de servicios previsto cuando la trama se reciba en el conmutador de borde correspondiente.

La Figura 5 proporciona un diagrama de flujo de un método 500 de ejemplo para modificar tramas para que incluyan un identificador específico del servicio. El método 500 puede implementarse mediante una puerta de enlace en las instalaciones de un usuario (p. ej., la puerta 210 de enlace).

El método 500 incluye una acción 501 de mantener, en el dispositivo de red, una tabla de ID que incluya entradas que asocien ID con criterios de coincidencia, incluyendo la tabla de ID una primera entrada que asocie un primer ID con un primer conjunto de criterios y una segunda entrada que asocie un segundo ID con un segundo conjunto de criterios. Por ejemplo, la puerta 210 de enlace puede mantener la tabla 300 de ID.

El método 500 incluye una acción 502 de recibir, a través de un puerto del dispositivo de red, una primera trama. Por ejemplo, la puerta 210 de enlace puede recibir una trama de la *smart TV* 100a que esté destinada al proveedor de vídeo en *streaming*.

El método 500 incluye una acción 503 de evaluar el contenido de la primera trama. Por ejemplo, la puerta 210 de enlace puede examinar una dirección MAC, una dirección IP, una etiqueta VLAN, un puerto TCP, etc. de la trama.

El método 500 incluye una acción 504 de comparar el contenido de la primera trama con las entradas de la tabla de ID. Por ejemplo, la puerta 210 de enlace puede evaluar el contenido de la trama frente a las entradas de la tabla 300 de ID.

El método 500 incluye una acción 505 de, al determinar que el contenido de la primera trama coincide con el primer conjunto de criterios, modificar la primera trama para que incluya el primer ID. Por ejemplo, la puerta 210 de enlace podría añadir ID1 como una etiqueta VLAN u otro tipo de ID a la trama cuando determine que la trama tiene una dirección MAC de origen de MAC1 y una dirección IP de destino de IP1.

El método 500 incluye una acción 506 de reenviar la primera trama modificada al conmutador o conmutadores de la red. Por ejemplo, la puerta 210 de enlace puede reenviar la trama con ID1 a través del puerto 212.

El método 500 incluye una acción 507 de recibir, a través del puerto, una segunda trama. Por ejemplo, la puerta 210 de enlace puede recibir una trama del sistema 100n de seguridad que esté destinada al proveedor de servicios de seguridad.

El método 500 incluye una acción 508 de evaluar el contenido de la segunda trama. Por ejemplo, la puerta 210 de enlace puede examinar una dirección MAC, una dirección IP, una etiqueta VLAN, un puerto TCP, etc. de la trama.

El método 500 incluye una acción 509 de comparar el contenido de la segunda trama con las entradas de la tabla de ID. Por ejemplo, la puerta 210 de enlace puede evaluar el contenido de la trama frente a las entradas de la tabla 300 de ID.

El método 500 incluye una acción 510 de, al determinar que el contenido de la segunda trama coincide con el segundo conjunto de criterios, modificar la segunda trama para que incluya el segundo ID. Por ejemplo, la puerta 210 de enlace podría añadir ID2 como una etiqueta VLAN u otro tipo de ID a la trama cuando determine que la trama tiene una dirección MAC de origen de MAC2 y una dirección IP de destino de IP2.

Finalmente, el método 500 incluye una acción 511 de reenviar la segunda trama modificada al conmutador o conmutadores de la red. Por ejemplo, la puerta 210 de enlace puede reenviar la trama con ID2 a través del puerto 212.

Las realizaciones de la presente invención pueden comprender o utilizar ordenadores de uso especial o de uso general, incluido hardware informático, tal como, por ejemplo, uno o más procesadores y memoria de sistema. Las realizaciones dentro del alcance de la presente invención también incluyen medios físicos y otros medios legibles por ordenador para transportar o almacenar instrucciones y/o estructuras de datos ejecutables por ordenador. Dichos

medios legibles por ordenador pueden ser cualquier medio disponible al que pueda acceder un sistema informático de uso general o de uso especial.

Los medios legibles por ordenador se clasifican en dos categorías separadas: medios de almacenamiento informático y medios de transmisión. Los medios (dispositivos) de almacenamiento informático incluyen RAM, ROM, EEPROM, CD-ROM, unidades de estado sólido ("SSD") (p. ej., basadas en RAM), memoria flash, memoria de cambio de fase ("PCM") y otros tipos de memoria, otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio de almacenamiento similar que pueda usarse para almacenar medios de código de programa deseados en forma de instrucciones o estructuras de datos ejecutables por ordenador y al que pueda acceder un ordenador de uso general o de uso especial. Los medios de transmisión incluyen señales y ondas portadoras.

Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que, cuando son ejecutados por un procesador, hacen que un ordenador de uso general, un ordenador de uso especial o un dispositivo de procesamiento de uso especial lleve a cabo una determinada función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, código binario, instrucciones de formato intermedio tales como lenguaje ensamblador o código-P, o incluso código fuente.

Los expertos en la técnica apreciarán que la invención se puede poner en práctica en entornos informáticos de red con muchos tipos de configuraciones de sistemas informáticos, incluyendo ordenadores personales, ordenadores de sobremesa, ordenadores portátiles, procesadores de mensajes, dispositivos portátiles, sistemas multiprocesador, electrónica de consumo programable o basada en microprocesadores, PC de red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, tabletas, buscapersonas, rúteres, conmutadores y similares.

La invención también se puede practicar en entornos de sistemas distribuidos donde los sistemas informáticos locales y remotos, que están vinculados (ya sea mediante enlaces de datos cableados, enlaces de datos inalámbricos o mediante una combinación de enlaces de datos cableados e inalámbricos) a través de una red, ambos llevan a cabo tareas. En un entorno de sistema distribuido, los módulos de programa pueden estar ubicados en dispositivos de almacenamiento de memoria tanto locales como remotos. Un ejemplo de un entorno de sistema distribuido es una nube de servidores en red o recursos de servidor. Por consiguiente, la presente invención se puede alojar en un entorno de nube.

La presente invención puede realizarse de otras formas específicas sin apartarse de la invención reivindicada. Las realizaciones descritas deben considerarse en todos los aspectos únicamente como ilustrativas y no restrictivas. Por lo tanto, el alcance de la invención reivindicada se indica en las reivindicaciones adjuntas y no en la descripción anterior.

REIVINDICACIONES

1. Un método, llevado a cabo por un dispositivo de red que incluye un puerto de salida mediante el cual el dispositivo de red está conectado a uno o más conmutadores de una red y un puerto de entrada al que están conectados una pluralidad de dispositivos conectables a la red en las instalaciones de un usuario, proporcionando cada uno de la pluralidad de dispositivos conectables a la red acceso a uno o más servicios en las instalaciones del usuario, el método para modificar tramas recibidas en el puerto de entrada para que incluyan un identificador específico del servicio, comprendiendo el método:
 - 5 mantener, en el dispositivo de red, una tabla de ID que incluya entradas que asocien ID con criterios de coincidencia, incluyendo los criterios de coincidencia una dirección MAC de origen y una dirección IP de destino, incluyendo la tabla de ID una primera entrada que asocie un primer ID con un primer conjunto de criterios y una segunda entrada que asocie un segundo ID con un segundo conjunto de criterios;
 - 10 recibir, a través del puerto de entrada del dispositivo de red, una primera trama desde un primer dispositivo conectable a la red de la pluralidad de dispositivos conectables a la red en las instalaciones del usuario que están conectados al puerto de entrada del dispositivo de red, proporcionando el primer dispositivo conectable a la red acceso a un primer servicio en las instalaciones del usuario;
 - 15 evaluar el contenido de la primera trama, incluyendo evaluar la dirección MAC de origen y la dirección IP de destino definidas en la primera trama;
 - comparar el contenido de la primera trama con las entradas de la tabla de ID;
 - 20 al determinar que el contenido de la primera trama coincide con el primer conjunto de criterios, incluyendo determinar que la dirección MAC de origen y la dirección IP de destino definidas en la primera trama coinciden con la dirección MAC de origen y la dirección IP de destino incluidas en el primer conjunto de criterios, modificar la primera trama para que incluya el primer ID que es específico del primer servicio;
 - reenviar la primera trama modificada al conmutador o conmutadores de la red;
 - 25 recibir, a través del puerto de entrada del dispositivo de red, una segunda trama desde un segundo dispositivo conectable a la red de la pluralidad de dispositivos conectables a la red en las instalaciones del usuario que están conectados al puerto de entrada del dispositivo de red, proporcionando el segundo dispositivo conectable a la red acceso a un segundo servicio en las instalaciones del usuario;
 - evaluar el contenido de la segunda trama, incluyendo evaluar una dirección MAC de origen y una dirección IP de destino definidas en la segunda trama;
 - 30 comparar el contenido de la segunda trama con las entradas de la tabla de ID;
 - al determinar que el contenido de la segunda trama coincide con el segundo conjunto de criterios, incluyendo determinar que la dirección MAC de origen y la dirección IP de destino definidas en la segunda trama coinciden con una dirección MAC de origen y una dirección IP de destino incluidas en el segundo conjunto de criterios, modificar la segunda trama para que incluya el segundo ID que es específico del segundo servicio; y
 - 35 reenviar la segunda trama modificada al conmutador o conmutadores de la red.
2. El método de la reivindicación 1, en donde los criterios de coincidencia también incluyen uno o más de un identificador del puerto de entrada del dispositivo de red, una dirección IP de origen o una dirección MAC de destino.
3. El método de la reivindicación 1, en donde los criterios de coincidencia también incluyen cada uno de un identificador del puerto de entrada del dispositivo de red, una dirección IP de origen o una dirección MAC de destino.
- 40 4. El método de la reivindicación 1, en donde el dispositivo de red es una puerta de enlace y la pluralidad de dispositivos conectables a la red se conectan al puerto de entrada de la puerta de enlace a través de un concentrador (*hub*) o un router.
5. El método de la reivindicación 1, en donde los ID primero y segundo están asociados con diferentes puertos de un conmutador de borde al que están conectados un primer y un segundo proveedor de servicios respectivamente, proporcionando el primer proveedor de servicios el primer servicio y proporcionando el segundo proveedor de servicios el segundo servicio.
- 45 6. El método de la reivindicación 1, en donde los ID son etiquetas VLAN.
7. El método de la reivindicación 1, en donde los primeros criterios identifican el primer dispositivo conectable a la red que envió la primera trama y un primer proveedor de servicios al que se dirige la primera trama, proporcionando el primer proveedor de servicios el primer servicio, y los segundos criterios identifican el segundo dispositivo conectable a la red que envió la segunda trama y un segundo proveedor de servicios al que se dirige la segunda trama,
- 50

proporcionando el segundo proveedor de servicios el segundo servicio.

8. El método de la reivindicación 7, en donde los primeros criterios identifican el primer dispositivo conectable a la red utilizando la dirección MAC del primer dispositivo conectable a la red y los segundos criterios identifican el segundo dispositivo conectable a la red utilizando la dirección MAC del segundo dispositivo conectable a la red.

5 9. El método de la reivindicación 8, en donde los primeros criterios identifican al primer proveedor de servicios utilizando la dirección IP del primer proveedor de servicios y los segundos criterios identifican al segundo proveedor de servicios utilizando la dirección IP del segundo proveedor de servicios.

10. El método de la reivindicación 1, en donde los criterios de coincidencia incluyen un puerto de capa tres.

10 11. Uno o más medios de almacenamiento informático que almacenan instrucciones ejecutables por ordenador que, cuando son ejecutadas por una puerta de enlace que incluye un puerto de salida mediante el cual la puerta de enlace está conectada a uno o más conmutadores de una red y un puerto de entrada al que están conectados una pluralidad de dispositivos conectables a la red en las instalaciones del usuario, proporcionando cada uno de la pluralidad de dispositivos conectables a la red acceso a uno o más servicios en las instalaciones del usuario, implementan un método para modificar las tramas recibidas en el puerto de entrada de la puerta de enlace para que incluyan un
15 identificador específico del servicio, comprendiendo el método:

mantener, en la puerta de enlace, una tabla de ID que incluya entradas que asocien ID con criterios de coincidencia, incluyendo los criterios de coincidencia una dirección MAC de origen y una dirección IP de destino, incluyendo la tabla de ID una primera entrada que asocie un primer ID con un primer conjunto de criterios y una segunda entrada que asocie un segundo ID con un segundo conjunto de criterios;

20 recibir, a través del puerto de entrada de la puerta de enlace, una primera trama desde un primer dispositivo conectable a la red de la pluralidad de dispositivos conectables a la red en las instalaciones del usuario que están conectados al puerto de entrada de la puerta de enlace, proporcionando el primer dispositivo conectable a la red acceso a un primer servicio en las instalaciones del usuario;

25 evaluar el contenido de la primera trama, incluyendo evaluar la dirección MAC de origen y la dirección IP de destino definidas en la primera trama;

comparar el contenido de la primera trama con las entradas de la tabla de ID;

30 al determinar que el contenido de la primera trama coincide con el primer conjunto de criterios, incluyendo determinar que la dirección MAC de origen y la dirección IP de destino definidas en la primera trama coinciden con una dirección MAC de origen y una dirección IP de destino incluidas en el primer conjunto de criterios, modificar la primera trama para que incluya el primer ID que es específico del primer servicio;

reenviar la primera trama modificada al conmutador o conmutadores de la red;

35 recibir, a través del puerto de entrada de la puerta de enlace, una segunda trama desde un segundo dispositivo conectable a la red de la pluralidad de dispositivos conectables a la red en las instalaciones del usuario que están conectados al puerto de entrada de la puerta de enlace, proporcionando el segundo dispositivo conectable a la red acceso a un segundo servicio en el domicilio del usuario;

evaluar el contenido de la segunda trama, incluyendo evaluar una dirección MAC de origen y una dirección IP de destino definidas en la segunda trama;

comparar el contenido de la segunda trama con las entradas de la tabla de ID;

40 al determinar que el contenido de la segunda trama coincide con el segundo conjunto de criterios, incluyendo determinar que la dirección MAC de origen y la dirección IP de destino definidas en la segunda trama coinciden con una dirección MAC de origen y una dirección IP de destino incluidas en el segundo conjunto de criterios, modificar la segunda trama para que incluya el segundo ID que es específico del segundo servicio; y

reenviar la segunda trama modificada al conmutador o conmutadores de la red.

45 12. El medio de almacenamiento informático de la reivindicación 11, en donde los criterios de coincidencia también incluyen uno o más de un identificador del puerto de entrada de la puerta de enlace, una dirección IP de origen o una dirección MAC de destino.

50 13. El medio de almacenamiento informático de la reivindicación 11, en donde el primer y el segundo ID están asociados con diferentes puertos de un conmutador de borde al que están conectados un primer y un segundo proveedor de servicios respectivamente, proporcionando el primer proveedor de servicios el primer servicio y proporcionando el segundo proveedor de servicios el segundo servicio.

14. El medio de almacenamiento informático de la reivindicación 11, en donde los primeros criterios identifican el

primer dispositivo conectable a la red que envió la primera trama y a un primer proveedor de servicios al que se dirige la primera trama, proporcionando el primer proveedor de servicios el primer servicio, y los segundos criterios identifican el segundo dispositivo conectable a la red que envió la segunda trama y a un segundo proveedor de servicios al que se dirige la segunda trama, proporcionando el segundo proveedor de servicios el segundo servicio.

- 5 15. El medio de almacenamiento informático de la reivindicación 14, en donde los primeros criterios identifican el primer dispositivo conectable a la red utilizando la dirección MAC del primer dispositivo conectable a la red y los segundos criterios identifican el segundo dispositivo conectable a la red utilizando la dirección MAC del segundo dispositivo conectable a la red; y

10 en donde los primeros criterios identifican al primer proveedor de servicios utilizando la dirección IP del primer proveedor de servicios y los segundos criterios identifican al segundo proveedor de servicios utilizando la dirección IP del segundo proveedor de servicios.

16. El medio de almacenamiento informático de la reivindicación 11, en donde el método comprende además: agregar una entrada a la tabla de ID en respuesta a que el usuario se suscriba a otro servicio proporcionado a través de la red, definiendo la entrada agregada un ID único y criterios asociados.

- 15 17. El medio de almacenamiento informático de la reivindicación 11, en donde el método comprende además:

recibir tramas de la red; y

eliminar un ID de cada una de las tramas recibidas antes de reenviar las tramas a través del puerto de entrada de la puerta de enlace.

18. Un sistema que comprende una arquitectura de red definida por software, comprendiendo el sistema:

20 una puerta de enlace que incluye un puerto de salida mediante el cual la puerta de enlace está conectada a uno o más conmutadores de una red y un puerto de entrada al que están conectados una pluralidad de dispositivos conectables a la red en las instalaciones de un usuario, proporcionando cada uno de la pluralidad de dispositivos conectables a la red acceso a uno o más servicios en las instalaciones del usuario; y

25 un conmutador de borde que incluye un primer puerto y un segundo puerto, conectando el primer puerto una primera red de proveedor de servicios al conmutador o conmutadores de la red, conectando el segundo puerto una segunda red de proveedor de servicios al conmutador o conmutadores de la red;

en donde la puerta de enlace está configurada para llevar a cabo el siguiente método para modificar las tramas recibidas en el puerto de entrada para que incluyan un identificador específico del servicio:

30 mantener una tabla de ID que incluya entradas que asocien ID con criterios de coincidencia, incluyendo los criterios de coincidencia una dirección MAC de origen y una dirección IP de destino, incluyendo la tabla de ID una primera entrada que asocie un primer ID con un primer conjunto de criterios y una segunda entrada que asocie un segundo ID con un segundo conjunto de criterios;

35 recibir, a través del puerto de entrada de la puerta de enlace, una primera trama desde un primer dispositivo conectable a la red de la pluralidad de dispositivos conectables a la red en las instalaciones del usuario que están conectados al puerto de entrada de la puerta de enlace, proporcionando el primer dispositivo conectable a la red acceso a un primer servicio en las instalaciones del usuario;

evaluar el contenido de la primera trama, incluyendo evaluar la dirección MAC de origen y la dirección IP de destino definidas en la primera trama;

comparar el contenido de la primera trama con las entradas de la tabla de ID;

40 al determinar que el contenido de la primera trama coincide con el primer conjunto de criterios, incluyendo determinar que la dirección MAC de origen y la dirección IP de destino definidas en la primera trama coinciden con una dirección MAC de origen y una dirección IP de destino incluidas en el primer conjunto de criterios, modificar la primera trama para que incluya el primer ID, estando el primer ID asociado con el primer puerto del conmutador de borde;

45 reenviar la primera trama modificada al conmutador o conmutadores de la red;

recibir, a través del puerto de entrada de la puerta de enlace, una segunda trama desde un segundo dispositivo conectable a la red de la pluralidad de dispositivos conectables a la red en las instalaciones del usuario que están conectados al puerto de entrada de la puerta de enlace, proporcionando el segundo dispositivo conectable a la red acceso a un segundo servicio en las instalaciones del usuario;

50 evaluar el contenido de la segunda trama, incluyendo evaluar una dirección MAC de origen y una dirección IP de destino definidas en la segunda trama;

comparar el contenido de la segunda trama con las entradas de la tabla de ID;

al determinar que el contenido de la segunda trama coincide con el segundo conjunto de criterios, incluyendo determinar que la dirección MAC de origen y la dirección IP de destino definidas en la segunda trama coinciden con una dirección MAC de origen y una dirección IP de destino incluidas en el segundo conjunto de criterios, modificar la segunda trama para que incluya el segundo ID, estando el segundo ID asociado con el segundo puerto del conmutador de borde; y

reenviar la segunda trama modificada al conmutador o conmutadores de la red.

19. El sistema de la reivindicación 18, en donde el conmutador de borde está configurado para reenviar las tramas que se reciben desde el conmutador o conmutadores de la red a través del primer puerto del conmutador de borde cuando las tramas tengan el primer ID y para reenviar las tramas que se reciben desde el conmutador o conmutadores de la red a través del segundo puerto del conmutador de borde cuando las tramas tengan el segundo ID.

20. El sistema de la reivindicación 18, en donde los criterios de coincidencia para al menos una de las entradas incluyen información de capa dos y capa tres.

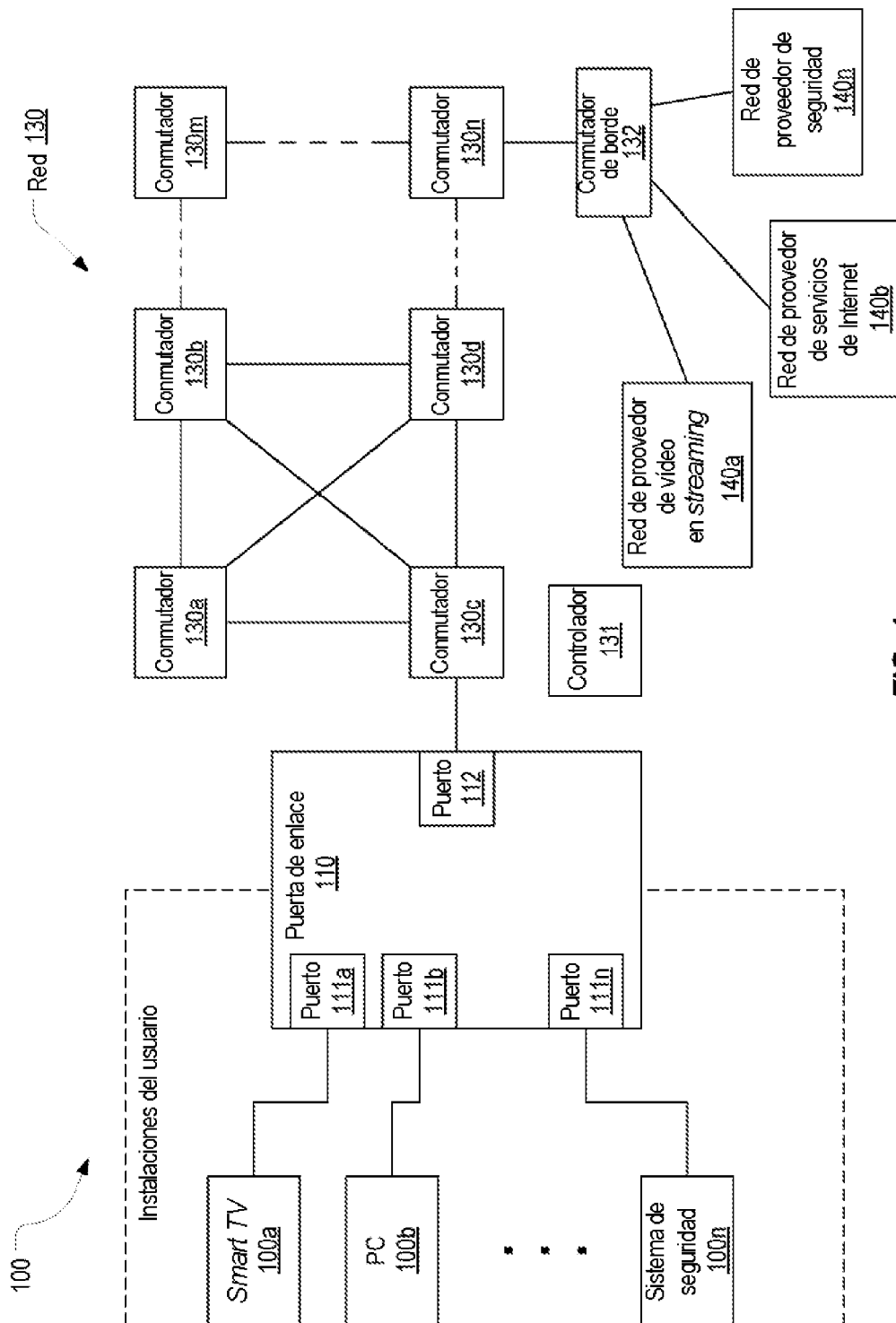


FIG. 1

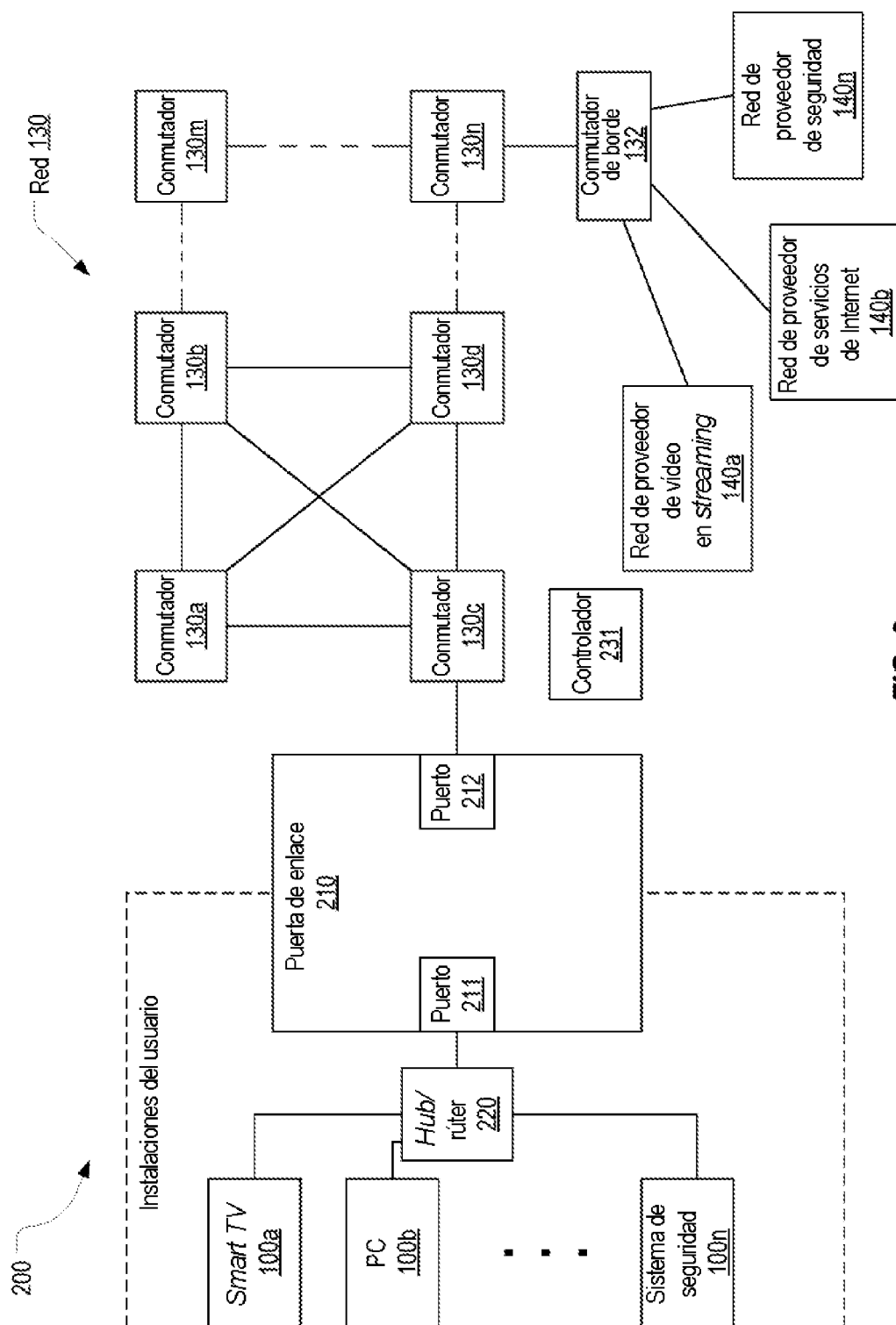


FIG. 2

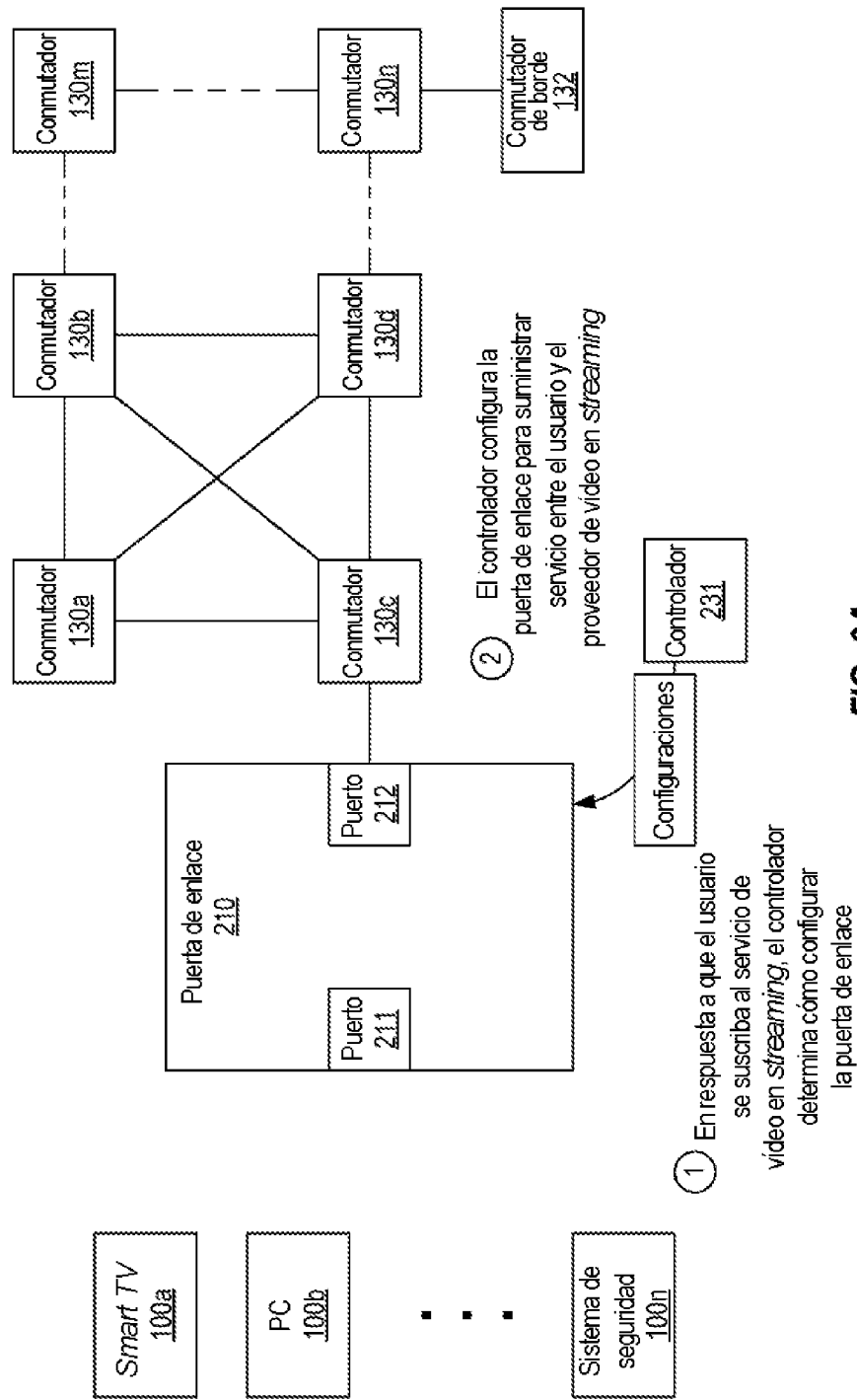


FIG. 3A

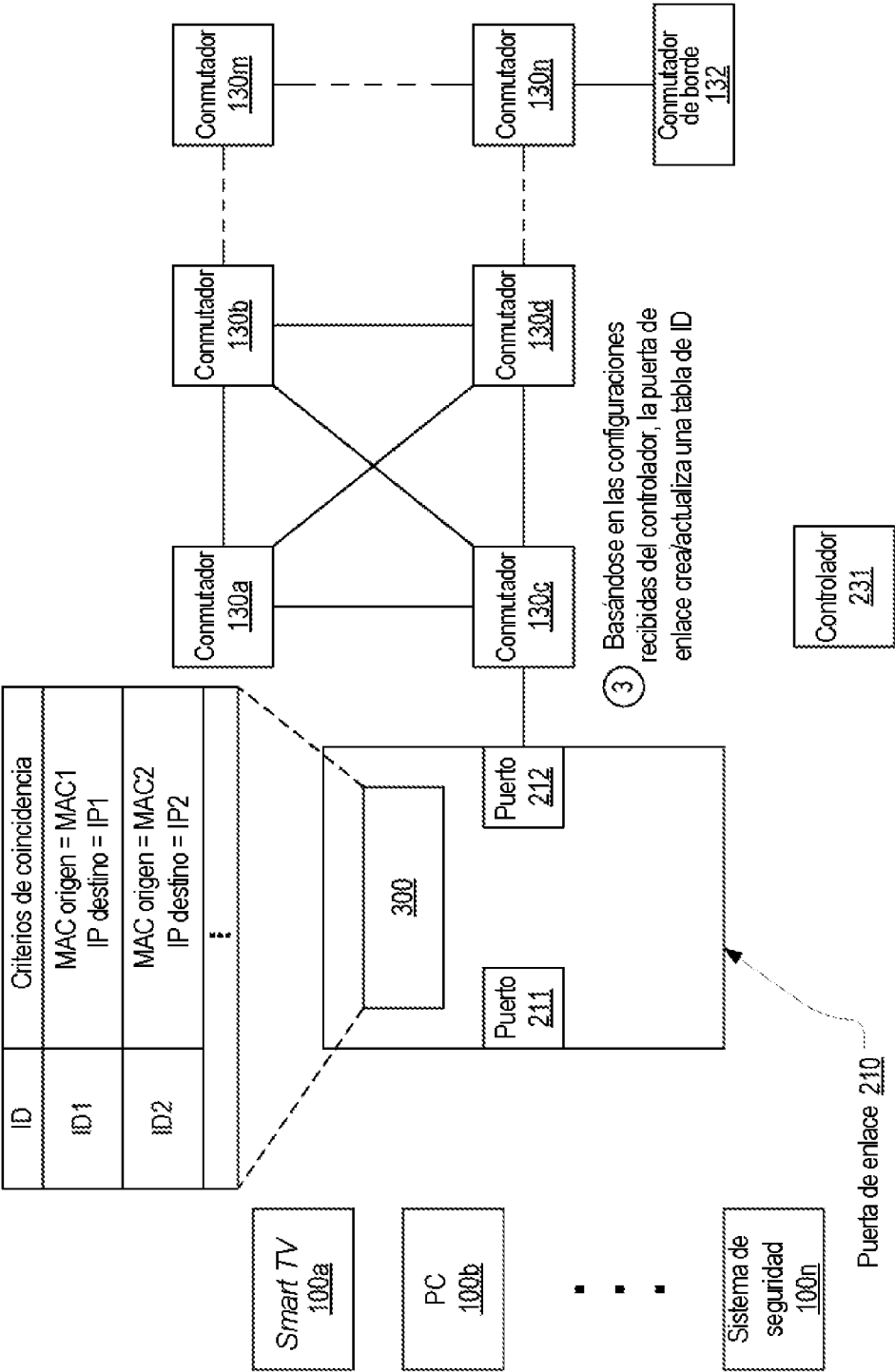


FIG. 3B

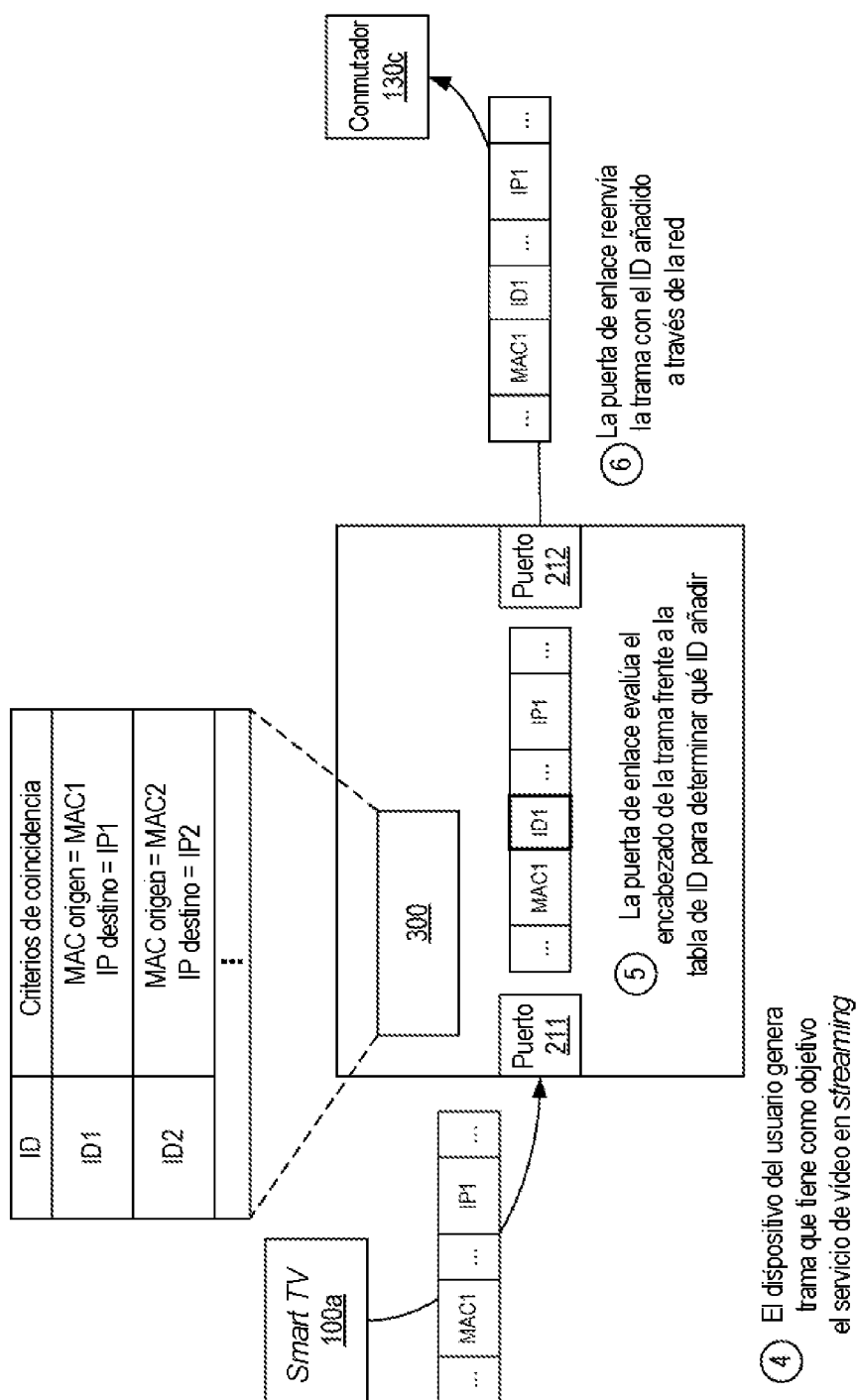


FIG. 3C

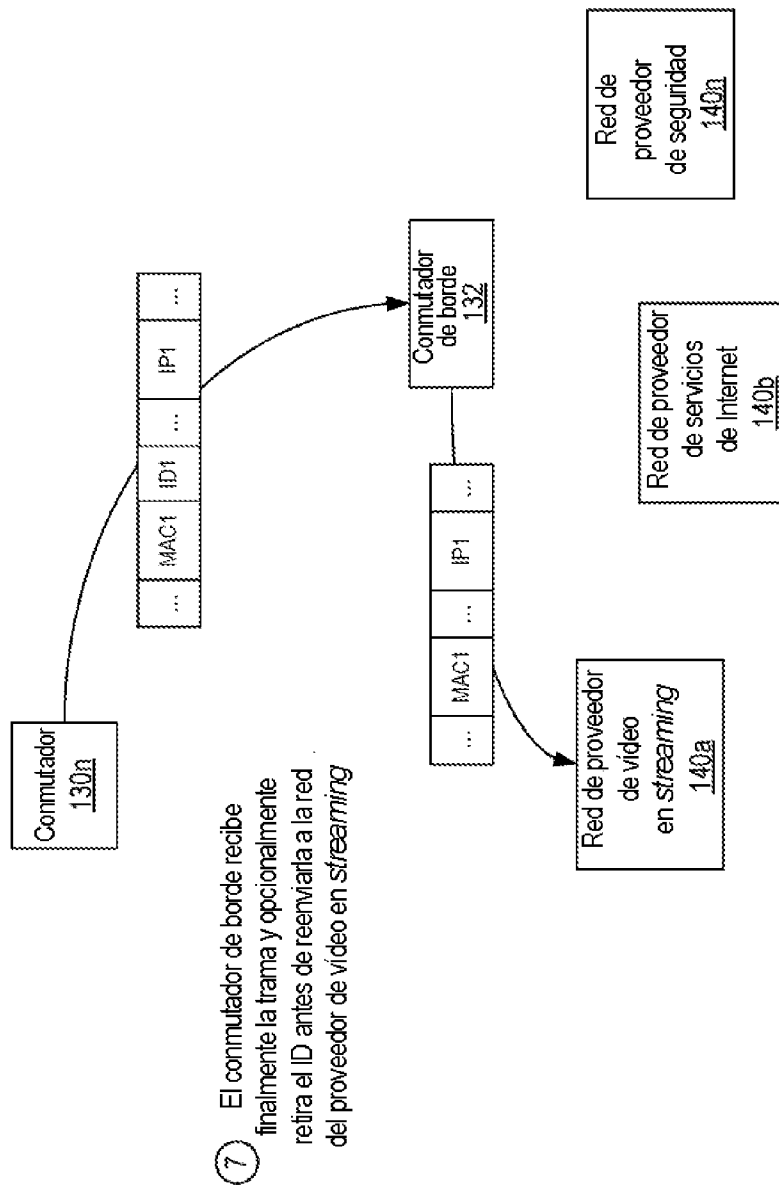


FIG. 3D

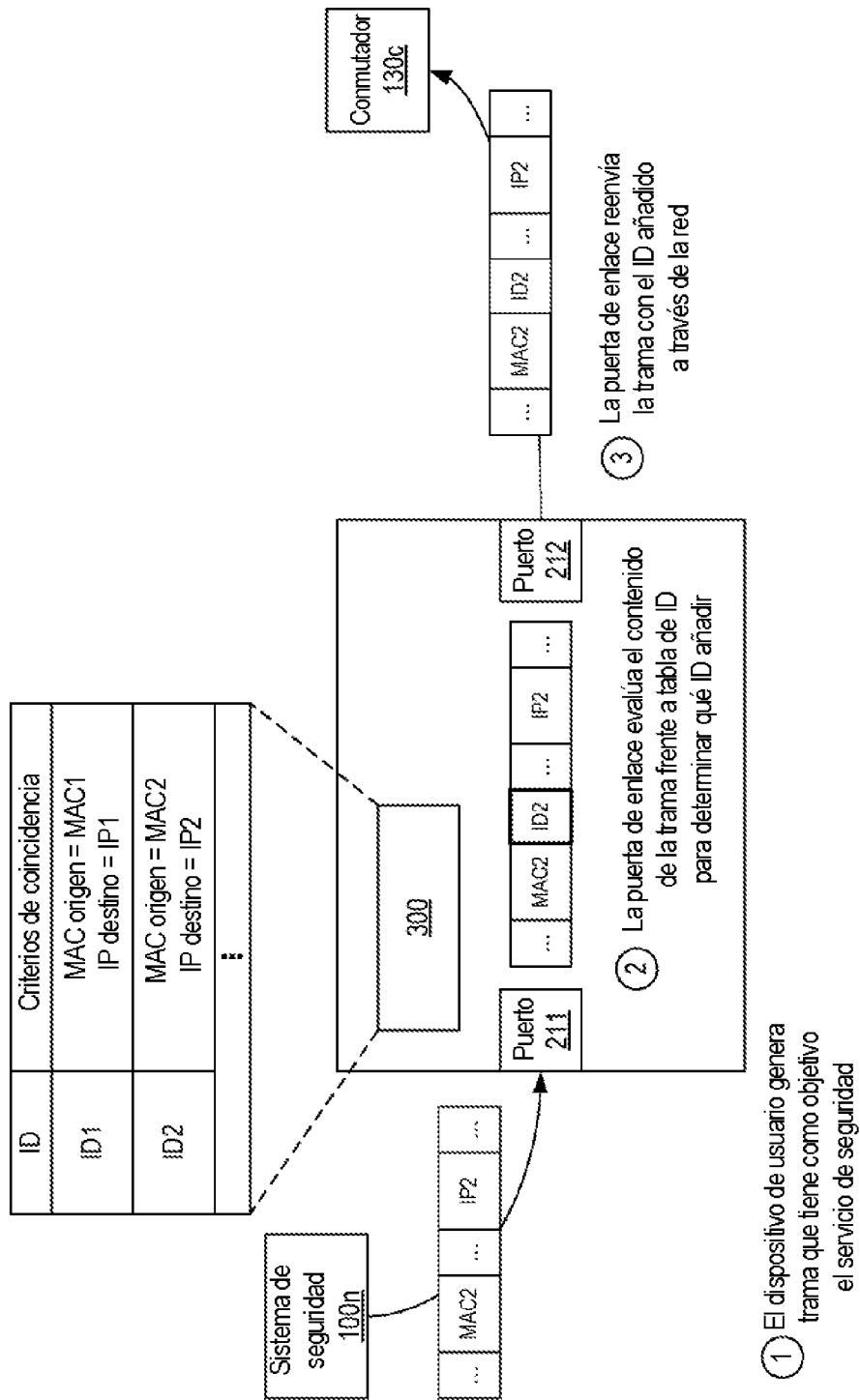


FIG. 4

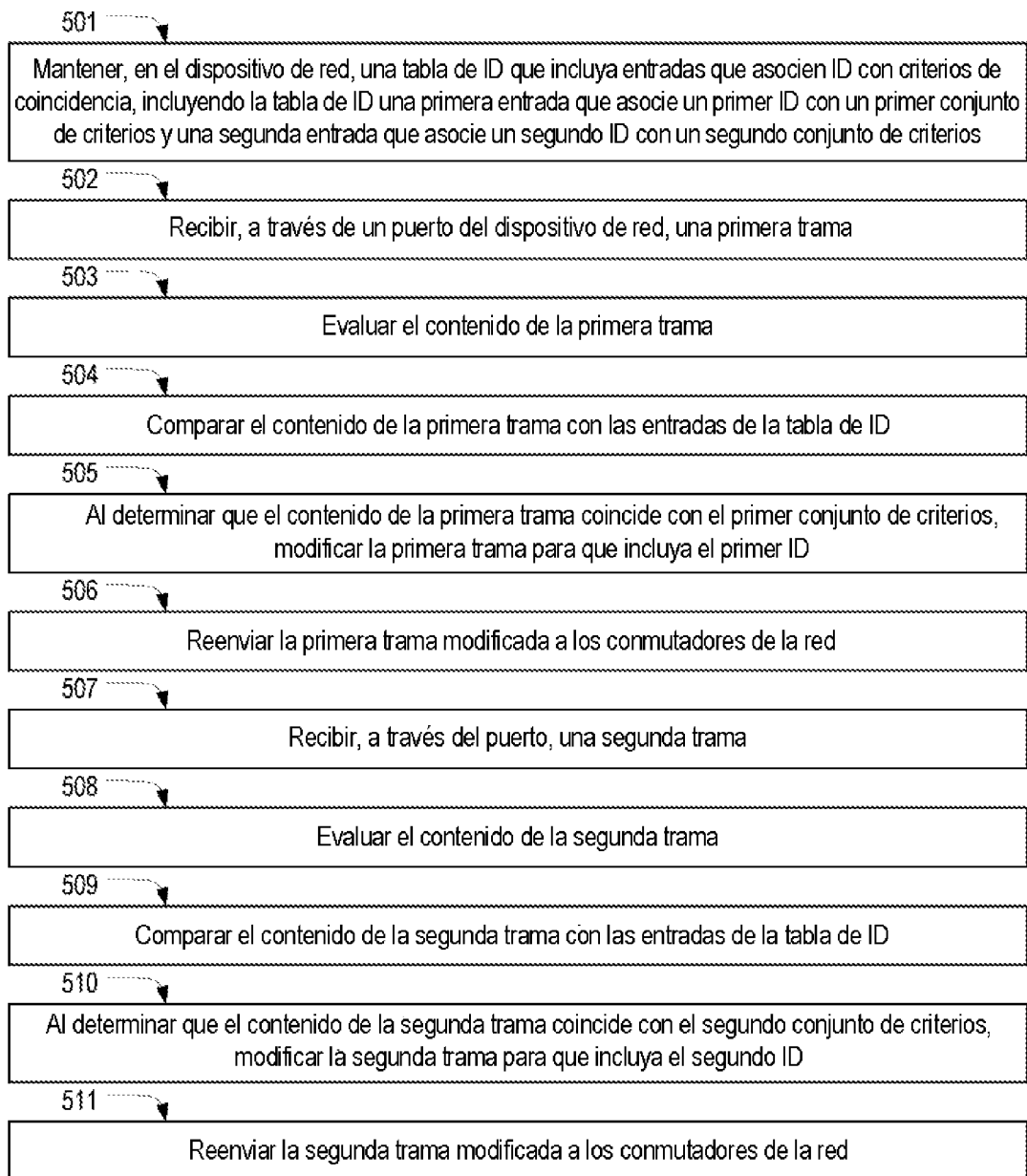


FIG. 5