(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 742 425**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 12/851 (2013.01)
H04W 28/10 (2009.01)
H04W 72/10 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.07.2010 E 15179533 (3)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2019 EP 2996282**

(54) Título: **Manejo del tráfico de red a través de un acceso fijo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.02.2020

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

LUDWIG, REINER y
EKSTRÖM, HANNES

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Manejo del tráfico de red a través de un acceso fijo

Sector técnico

La presente invención se refiere a métodos y dispositivos para el manejo de tráfico de red a través de un acceso fijo.

Antecedentes

En las redes de comunicación, la separación del tráfico es un concepto que permite que diferentes tipos de tráfico en tráficos reciban diferente tratamiento en las funciones de transmisión del tráfico del plano de usuario, por ejemplo, con respecto a la puesta en cola, al control del error de planificación, o a otros similares. Para implementar la separación de tráfico, un nodo de frontera puede clasificar los paquetes en diferentes clases de tráfico, por ejemplo, tráfico de voz, trafico multimedia o tráfico de internet. Sobre la base de esta clasificación, los paquetes de datos pueden ser provistos de un marcado que permite a la función de transmisión del tráfico del plano de usuario asociar los paquetes de datos con la respectiva clase de tráfico y el tratamiento de transmisión asociado.

Si el nodo de frontera es una puerta de enlace residencial que comunica el tráfico de datos con la red a través de un acceso fijo, por ejemplo, utilizando una línea de abonado digital (DSL – Digital Subscriber Line, en inglés) o tecnología de cable coaxial, es conocido realizar una clasificación del tráfico en la dirección de enlace ascendente, es decir, de la puerta de enlace residencial a la red, sobre la base del mapeo de puertos. En este caso, la puerta de enlace residencial está provista de múltiples puertos físicos que están cada uno dedicados a un cierto tipo de dispositivo final, por ejemplo, un puerto de voz para conectarse a un teléfono fijo, un puerto de TV para conectarse a una TV digital o a un decodificador digital, y un puerto de internet para conectarse a un ordenador o a otro tipo de dispositivo de internet de propósito múltiple. El puerto de internet puede ser asimismo acoplado a un punto de acceso de una red de área local inalámbrica (WLAN – Wireless Local Area Network, en inglés), en ocasiones denominada punto de acceso WiFi. En tal escenario, todo el tráfico recibido en el puerto de voz puede ser clasificado como tráfico de voz, todo el tráfico recibido en el puerto de TV puede ser clasificado como tráfico multimedia y todo el tráfico recibido en el puerto de internet puede ser clasificado como tráfico de internet. A los paquetes de datos del tráfico clasificado puede a continuación proporcionárseles el marcado correspondiente para ser utilizados en la transmisión de enlace ascendente por medio de acceso fijo.

Como alternativa, la clasificación del tráfico puede basarse en una configuración semiestática de la puerta de enlace residencial. Por ejemplo, todo el tráfico de datos enviado a una cierta dirección de protocolo de internet (IP – Internet Protocol, en inglés) o a un cierto rango de direcciones de IP puede ser asignado a una cierta clase de tráfico. Este planteamiento puede ser asimismo aplicado cuando el nodo de frontera es un terminal móvil que se comunica con un nodo de acceso fijo utilizando tecnología de acceso inalámbrico. Además, las reglas de clasificación podrían ser señaladas desde la red al nodo de frontera.

No obstante, utilizar los conceptos anteriores para efectuar la clasificación del tráfico puede resultar difícil para que un operador de red gestione de manera eficiente un gran número de nodos de frontera de tal manera que la clasificación del tráfico se realice de manera deseada.

El documento US 6.286.052 B1 describe un sistema dentro de una red informática que identifica flujos de tráfico específicos que se originan desde una entidad de red determinada y solicita y aplica reglas de política apropiadas o tratamientos de servicio a los flujos de tráfico. Una entidad de red incluye un componente de declaración de flujo que se comunica con uno o más programas de aplicación que se ejecutan en la entidad. El componente de declaración de flujo incluye un generador de mensajes y una memoria asociada para almacenar una o más estructuras de datos de flujo de tráfico. Para un flujo de tráfico determinado, el programa de aplicación emite una o más llamadas al componente de declaración de flujo que le proporciona información que identifica los flujos de tráfico. El componente de declaración de flujo abre entonces una sesión de gestión de flujo con un ejecutor de políticas local que obtiene reglas de políticas o tratamientos de servicio para el flujo identificado de un servidor de políticas y aplica esas reglas o tratamientos a los flujos de tráfico específicos desde la entidad de red.

De acuerdo con esto, existe la necesidad de técnicas potentes y eficientes para el manejo del tráfico de red por a través de un acceso fijo.

Sumario

Se proporcionan un método, un dispositivo de comunicación y un producto de programa informático de acuerdo con las reivindicaciones independientes.

De acuerdo con una realización de la invención, se proporciona un método de manejo del tráfico de red en un dispositivo de comunicación. De acuerdo con el método, los paquetes de datos entrantes se reciben a través de un acceso fijo en el dispositivo de comunicación. Los paquetes de datos incluyen un primer identificador y son marcados de acuerdo con una clase de tráfico. En los paquetes de datos salientes que se transmitirán a través del acceso fijo desde el dispositivo de comunicación, se detectan paquetes de datos que incluyen un segundo

identificador que es complementario con respecto al citado primer identificador. Los paquetes de datos salientes detectados que tienen el citado segundo identificador son asignados a la misma clase de tráfico que los paquetes de datos entrantes que tienen el citado primer identificador.

De acuerdo con otra realización de la invención, se proporciona un dispositivo de comunicación. El dispositivo de comunicación incluye una interfaz configurada para recibir paquetes de datos entrantes a través de un acceso fijo desde una red y una interfaz configurada para enviar paquetes de datos salientes a través del acceso fijo a la red. El dispositivo de comunicación incluye además un clasificador de tráfico. El clasificador de tráfico está configurado para detectar paquetes de datos entrantes que incluyen un primer identificador y paquetes de datos de salientes que incluyen un segundo identificador que es complementario del citado primer identificador. Además, el clasificador de tráfico está configurado para marcar los citados paquetes de datos salientes que tienen el citado segundo clasificador complementario a la misma clase de tráfico que los paquetes de datos entrantes que tienen el primer identificador.

De acuerdo con otras realizaciones de la invención, pueden proporcionarse otros métodos o dispositivos. Asimismo, de acuerdo con una realización de la invención, se puede proporcionar un producto de programa informático que comprende código de programa que, cuando es ejecutado por un procesador de un dispositivo de comunicación, hace que el dispositivo de comunicación opere de acuerdo con el método anterior.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente un entorno de red de comunicación en el cual pueden aplicarse conceptos de acuerdo con realizaciones de la invención.

La Figura 2 ilustra esquemáticamente un sistema de comunicación en el cual pueden aplicarse conceptos de acuerdo con realizaciones de la invención.

La Figura 3 ilustra esquemáticamente un ejemplo de un paquete de datos tal como el utilizado en una realización de la invención.

La Figura 4 ilustra esquemáticamente otro ejemplo de un paquete de datos tal como se utiliza en una realización de la invención.

La Figura 5 ilustra esquemáticamente un identificador y un identificador complementario en paquetes de datos.

La Figura 6 ilustra esquemáticamente un campo de información en una sección de cabecera de paquetes de datos.

La Figura 7 ilustra esquemáticamente una trama de protocolo que soporta el marcado de paquetes de datos.

La Figura 8 ilustra esquemáticamente una implementación de un dispositivo de comunicación de acuerdo con una realización de la invención.

La Figura 9 muestra un diagrama de flujo para ilustrar un método de manejo del tráfico de datos de UL de acuerdo con una realización de la invención.

Descripción detallada de las realizaciones

En lo que sigue, la invención se explicará con más detalle por referencia a realizaciones de ejemplo y a los dibujos que se acompañan. Las realizaciones ilustradas se refieren al manejo del tráfico de datos de enlace ascendente (UL) de un dispositivo de comunicación, es decir, al tráfico de datos desde el dispositivo de comunicación a una red de comunicación. La red de comunicación proporciona un acceso a través de un acceso fijo, es decir, implementado utilizando tecnología de acceso de DSL, tecnología de acceso óptica o tecnología de acceso por cable coaxial. Además, la red de comunicación puede proporcionar asimismo un acceso a través de un nodo de acceso por radio de una red de radio móvil celular. Por ejemplo, la red de radio móvil celular puede ser implementada de acuerdo con las especificaciones técnicas del 3GPP (Proyecto de Colaboración de Tercera Generación – Third Generation Partnership Project, en inglés), por ejemplo como una red del sistema global para comunicaciones móviles (GSM – Global System por Mobile Communications, en inglés), como la red del sistema de telecomunicaciones móviles universal (UMTS – Universal Mobile Telecommunications System, en inglés), o como una red de evolución de arquitectura de servicio (SAE – Serving Architecture Evolution, en inglés) / Evolución a largo plazo (LTE – Long Term Evolution, en inglés). No obstante, debe entenderse que los conceptos tal como los descritos en esta memoria pueden ser asimismo aplicados a otros tipos de redes de comunicación. Las realizaciones tal como las descritas en esta memoria efectúan la clasificación del tráfico de UL sobre la base de las reglas de clasificación del tráfico de UL que son localmente generadas mediante la monitorización del tráfico de datos de enlace descendente (DL), en particular información en las cabeceras de protocolo de los paquetes de datos de DL.

La Figura 1 ilustra esquemáticamente un entorno de red de comunicación en el cual pueden aplicarse conceptos de acuerdo con realizaciones de la invención. Como se ilustra, el entorno de red de comunicación incluye un dominio de red de radio móvil celular 10 de acuerdo con las especificaciones técnicas del 3GPP. Además, se proporciona un dominio de acceso fijo 20. Además, el entorno de red de comunicación incluye un dominio local 30, que incluye

varios dispositivos de casa del abonado acoplados al dominio de acceso fijo 20. Los componentes del dominio local 30 están típicamente situados en casa del abonado. En el dominio local, se proporciona una puerta de enlace residencial (RG – Residential Gateway, en inglés) 35, que es un dispositivo de comunicación en casa del abonado, que se utiliza para acoplar los dispositivos de casa del abonado al dominio de acceso fijo 20. En particular, la RG 35 puede acoplar una red de área local (LAN) en casa del abonado al dominio de acceso fijo 20 de la red de comunicación.

En el ejemplo ilustrado, el dominio de red de radio móvil celular 10 es implementado de acuerdo con SAE / LTE del 3GPP. Como se ilustra, el dominio de red de radio móvil celular 10 incluye una puerta de enlace de red de radio de datos en paquetes (PDN GW – Packet Data Network Gateway, en inglés) que está acoplada a las redes de acceso por radio (RAN – Radio Access Network, en inglés) a través de una puerta de enlace de servicio (SGW – Serving GateWay, en inglés). Como se ilustra, las RAN pueden incluir una o más RAN de EDGE de GSM (GERAN – GSM EDGE RAN, en inglés), RAN terrestre de UMTS (UTRAN – UMTS Terrestrial RAN, en inglés) o UTRAN evolucionada (E-UTRAN – Evolved UTRAN, en inglés). En el dominio de red de radio móvil celular 10, los servicios de IP del operador, por ejemplo los servicios del subsistema Multimedia de IP (IMS – IP Multimedia Subsystem, en inglés) pueden ser albergados por los servidores de aplicación u otros. Un terminal móvil o equipo de usuario (UE – User Equipment, en inglés) 40, por ejemplo, un teléfono móvil, un ordenador portátil u otros, pueden acceder a los servicios de IP del operador a través de la PDN GW.

Además, el dominio de red de radio móvil celular 10 incluye nodos de control, tales como la función de reglas de política y tarificación (PCRF – Policy and Charging Rules Function, en inglés) y una entidad de gestión de movilidad (MME – Mobility Management Entity, en inglés), una base de datos de abonados en forma de un servidor de abonados locales (HSS – Home Subscriber Server, en inglés) y un servidor de autenticación, autorización y contabilidad (AAA – Authentication, Authorization and Accounting, en inglés) del 3GPP.

Además, para soportar la tecnología de femto acceso del 3GPP, el dominio de red de radio móvil celular 10 incluye una puerta de enlace de eNodoB local (HeNB GW – Home eNodeB GateWay, en inglés) y una puerta de enlace de seguridad (Sec GW – Security Gateway, en inglés). Para el acoplamiento a dominios de red no 3GPP, por ejemplo al dominio de acceso fijo 20, el dominio de red de radio móvil celular 10 incluye además una puerta de enlace de datos en paquetes evolucionados (ePDG – Evolved Packet Data Gateway, en inglés). Pueden obtenerse más detalles relativos a los componentes anteriores del dominio de red de radio móvil celular 10 y de las interfaces proporcionadas entre estos componentes a partir de las especificaciones técnicas del 3GPP.

El dominio de acceso fijo 20 incluye una infraestructura de operador para proporcionar acceso fijo a la red de comunicación, por ejemplo, utilizando tecnología de acceso de DSL, tecnología de acceso óptico, o tecnología de acceso por cable coaxial. Para ello, se proporciona una puerta de enlace de red de banda ancha (BNG – Broadband Network Gateway, en inglés), que se comunica con la ePDG y/o con la PDN GW en el dominio de red de radio móvil celular 10. Además, la BNG se comunica con la RG 35 en el dominio local 30 utilizando enlaces de comunicación fijos, por ejemplo por hilo o por cable. Dependiendo de la tecnología de acceso utilizada con respecto a la RG 35, el dominio de acceso fijo 20 puede estar provisto del correspondiente nodo de acceso, por ejemplo, un multiplexador de acceso de DSL (DSLAM – DSL Access Multiplexer, en inglés), un terminal de red óptico (ONT – Optical Network Terminal, en inglés) o un extremo de cabecera de cable coaxial.

Además, el dominio de acceso fijo 20 incluye un nodo de control de políticas en forma de una función de políticas y tarificación de banda ancha (BPCF) y un servidor de autenticación, autorización y contabilidad (AAA) de acceso fijo (FA – Fixed Access, en inglés). El nodo de control de políticas en el dominio de red de radio móvil celular 10, es decir, la PCRF, se comunica con el nodo de control de políticas en el dominio de acceso fijo 20, es decir, la BPCF. Además, el servidor de AAA del 3GPP se comunica con el servidor de AAA de FA. Además, la BNG en el dominio de acceso fijo 20 se comunica con la Sec GW en el dominio de red de radio móvil celular 10. De este modo, es posible una interacción segura entre el dominio de red de radio móvil celular 10 y el dominio de acceso fijo 20.

El dominio local 30 incluye la RG 35 y un número de dispositivos de casa del abonado conectados al mismo. En el ejemplo ilustrado, los dispositivos de casa del abonado incluyen un dispositivo de entretenimiento digital en forma de centro de medios (MC – Media Center, en inglés), un dispositivo informático de propósito múltiple en forma de un ordenador personal (PC – Personal Computer, en inglés), un receptor de televisión (TV) acoplado a la RG 35 a través de un decodificador (STB – Set-Top-Box, en inglés), y puntos de acceso inalámbrico, en particular un punto de acceso (AP – Access Point, en inglés) WiFi y un punto de femto acceso (AP) del 3GPP.

En el entorno de red de comunicación de la Figura 1, el UE 40 puede moverse entre accesos en el dominio de red de radio móvil celular 10, por ejemplo, utilizando GERAN, UTRAN o E-UTRAN y entre accesos a través del dominio de acceso fijo 20, por ejemplo, a través del Femto AP o el WiFi AP del 3GPP. Esto se ilustra mediante una flecha de trazos.

La Figura 2 ilustra esquemáticamente un sistema de comunicación en el cual se maneja tráfico de datos de UL de acuerdo con una realización de la invención. El sistema de comunicación incluye un dispositivo de comunicación 100, un nodo de acceso fijo 250 y un nodo de red 220. Además, el sistema de comunicación incluye un nodo de control 300. El sistema de comunicación ilustrado puede ser parte del entorno de red de comunicación de la Figura

1. Por ejemplo, el dispositivo de comunicación 100 puede corresponder al UE 40 o a la RG 35. El nodo de red 220 puede corresponder a la BNG o a la PDN GW. Si el dispositivo de comunicación 100 corresponde a la RG 35, el nodo de acceso fijo 250 puede ser cualquier tipo de nodo de acceso acoplado entre la BNG y la RG 35 para implementar el acceso fijo entre la BNG y la RG. El nodo de acceso fijo 250 puede asimismo ser integrado en la BNG o en la RG 35. A modo de ejemplo, el nodo de acceso fijo 250 puede ser implementado por un DSLAM, una ONT, un modem de cable u otros. El nodo de acceso fijo 250 puede estar situado en el dominio de acceso fijo 20 o en el dominio local 10. Si el dispositivo de comunicación 100 corresponde al UE 40, el nodo de acceso fijo puede ser también la RG 35. De acuerdo con esto, el dispositivo de comunicación 100 puede ser un UE acoplado al nodo de red 220 a través de una puerta de enlace residencial o puede ser la propia puerta de enlace residencial. La puerta de enlace residencial tiene un enlace de comunicación fijo al nodo de red, mientras que el enlace de comunicación entre el UE y la puerta de enlace residencial puede ser inalámbrico. La puerta de enlace residencial es autenticada típicamente utilizando el enlace de comunicación fijo al nodo de red 220, que para este propósito puede comunicarse con un servidor de autenticación, por ejemplo, el servidor FA AAA de la Figura 1. Si un UE se conecta a través de la puerta de enlace residencial al nodo de red 220, entonces una autenticación independiente del UE en un dominio de acceso fijo no es necesaria. El nodo de control 300 puede ser la BPCF o la PCRF.

Como se ilustra además, el dispositivo de comunicación 100 y el nodo de red 220 comunican paquetes de datos en la dirección de DL y en la dirección de UL. Los paquetes de datos son asignados a diferentes clases de tráfico 50, lo que se ilustra esquemáticamente mediante flechas de doble punta separadas. Las clases de tráfico puede ser, por ejemplo, tráfico de voz, tráfico multimedia y tráfico de internet. Para cada una de las clases de tráfico 50 puede definirse un tratamiento de transmisión correspondiente en los nodos intermedios, por ejemplo, el nodo de acceso fijo 250 o un nodo de transporte (no ilustrado). Cada clase de tráfico 50 puede corresponder a un cierto nivel de calidad de servicio (QoS – Quality of Service, en inglés). Por ejemplo, la clase de tráfico de voz puede tener un nivel de QoS más elevado que la clase del tráfico de internet. De acuerdo con realizaciones de la presente invención, la clasificación del tráfico de datos de UL en el dispositivo de comunicación 100 se efectúa detectando identificadores de paquetes de datos de UL salientes que son complementarios de identificadores de paquetes de datos de DL entrantes. Los paquetes de datos de DL están ya asignados a las clases de tráfico 50, por ejemplo, mediante un clasificador de tráfico 210 del nodo de red 220, que opera sobre la base de reglas de clasificación de paquetes de DL 215. En el ejemplo ilustrado, el clasificador de tráfico 210 del nodo de red 220 está controlado por el nodo de control 300, por ejemplo, sobre la base de datos de políticas. Los paquetes de datos de UL salientes que contienen el identificador complementario son asignados a la misma clase de tráfico 50 que los paquetes de datos de DL entrantes. Para ello, el dispositivo de comunicación 100 está provisto de un clasificador de tráfico 110, que puede ser operado en un modo reflexivo. En el modo reflexivo, el clasificador de tráfico 110 monitoriza los paquetes de datos de DL con el fin de generar localmente reglas de clasificación de paquetes de UL 115.

En el dispositivo de comunicación 100, la clase de tráfico 50 a la cual están asignados los paquetes de datos de DL puede ser detectada sobre la base de un marcado de los paquetes de datos de DL. La monitorización de los paquetes de datos de DL puede ser efectuada identificando una fuente de los paquetes de datos de DL recibidos, por ejemplo, sobre la base de un identificador de fuente en los paquetes de datos. Por ejemplo, los identificadores de fuente pueden ser direcciones de IP de fuente. Esta información es utilizada a continuación para generar localmente las reglas de clasificación de paquetes de UL 115. Las reglas de clasificación de paquetes de UL operan para asignar los paquetes de datos de UL, que son dirigidos hacia la fuente identificada, a la misma clase de tráfico 50 que los paquetes de datos de DL de esta fuente. Los paquetes de datos de UL clasificados son marcados de acuerdo con la clase de tráfico a la cual son asignados, por ejemplo, utilizando el mismo marcado que en los paquetes de datos de DL.

En lo que sigue, el modo reflexivo del clasificador de tráfico 110 se explicará con más detalle por referencia a estructuras de ejemplo de paquetes de datos y tramas de protocolo utilizados en la transmisión de paquetes de datos.

La Figura 3 ilustra esquemáticamente los paquetes de datos de IP del tipo de versión 4 de IP. Como se ilustra, una sección de cabecera de los paquetes de datos incluye varios campos de información, que se denominan “Versión”, “IHL (Longitud de cabecera de IP)”, “Servicios diferenciados”, “Longitud total”, “Identificación”, “Marcas”, “Desplazamiento de fragmento”, “Tiempo de vida”, “Protocolo”, “Suma de control de cabecera”, “Dirección de fuente”, “Dirección de destino”, “Opciones” y “Rellenado”. Los detalles relativos a estos campos se definen en la especificación RFC 791. El campo de información denominado “Servicios diferenciados”, se define en la especificación RFC 2475. Además, la sección de cabecera de un paquete de datos de IP incluirá también campos de información que se denominan “Puerto de fuente” y “Puerto de destino”. Campos de información correspondientes se definen, por ejemplo, mediante el Protocolo de control de transporte (TCP – Transport Control Protocol, en inglés) definido en la especificación RFC 793 y en el Protocolo de diagrama de datos de usuario (UDP – User Datagram Protocol, en inglés) tal como se define en la especificación RFC 768.

A continuación de la sección de cabecera, los paquetes de datos de IP están provistos típicamente de una sección de datos, en la cual pueden incluirse diferentes tipos de tráfico de datos de carga útil.

La Figura 4 ilustra esquemáticamente paquetes de datos de IP de acuerdo con el tipo de versión 6 de IP. De nuevo, la sección de cabecera incluye un número de campos de información, que se denominan “Versión”, “Servicios

diferenciados", "Etiqueta de flujo", "Longitud de carga útil", "Siguiente cabecera", "Límite de salto", "Dirección de fuente" y "Dirección de destino". Esta estructura de la sección de cabecera se define en la especificación RFC 2460. Además, la sección de cabecera puede comprender también campos de información denominados "Puerto de fuente" y "Puerto de destino", por ejemplo, tal como se define mediante el TCP o el UDP. De nuevo, la sección de cabecera será seguida típicamente de una sección de datos que puede contener varios tipos de datos de carga útil.

Para los propósitos de la presente descripción, solo se explicarán con más detalle los campos de información denominados "Servicios diferenciados", "Dirección de fuente", "Dirección de destino", "Puerto de fuente" y "Puerto de destino". Por lo que respecta a los otros campos de información, pueden tomarse más explicaciones de las especificaciones RFC mencionadas anteriormente.

El campo de información "Dirección de fuente" indica la dirección de IP desde la cual se origina un paquete de datos. De manera similar, el campo de información "Dirección de destino" indica la dirección de IP a la cual está destinado el paquete de datos. En la versión 4 de IP, la dirección de fuente y la dirección de destino son valores de 32 bits. En la versión 6 de IP, la dirección de fuente y la dirección de destino son valores de 128 bits.

El campo de información "Puerto de fuente" indica un número de puerto en la fuente del paquete de datos, mientras que el campo de información "Puerto de destino" indica un número de puerto en el punto de destino del paquete de datos.

Sobre la base de la dirección de fuente, la dirección de destino, el puerto de fuente y el puerto de destino, un flujo de paquetes de IP puede definirse como un flujo de paquetes de IP entre un primer punto final definido por la dirección de fuente y el puerto de fuente, y un segundo punto final definido por la dirección de destino y el puerto de destino. Una entidad que incluye la dirección de fuente, la dirección de destino, el puerto de fuente, el puerto de destino y un identificador de protocolo se denominan también "tupla de orden 5 de IP".

El campo de información "Servicios diferenciados" se incluye tanto en los paquetes de datos de la versión 4 de IP como en los paquetes de datos de la versión 6 de IP. Como se define en la especificación RFC 2474, el campo de información "Servicios diferenciados" es un valor de 8 bits. La estructura de este campo de información se ilustra esquemáticamente en la Figura 5.

Como se ilustra en la Figura 5, se utilizan seis bits del campo de información, es decir, los bits 0 – 5, para definir el punto de código de servicios diferenciados (DSCP – Differentiated Services Code Point, en inglés). Los otros dos bits no se utilizan. Utilizando el DSCP, el envío de los paquetes de datos por parte de los nodos de red puede ser controlado. Para los paquetes de datos que pertenecen a diferentes tipos de servicios pueden seleccionarse diferentes procedimientos de envío. Los DSCP pueden ser estandarizados. Además, está disponible un rango de DSCP no estandarizado.

La Figura 6 ilustra esquemáticamente la estructura de un trama de protocolo de acuerdo con los estándares IEEE 802.1 q y 802.1 p. La trama de protocolo se utiliza en la capa de control de acceso a medios (MAC – Media Access Control, en inglés) y puede utilizarse para transmitir los paquetes de IP tal como se explica en conexión con las Figs. 3, 4 y 5. El paquete de datos de IP se incluiría entonces en un campo de datos de la trama de protocolo.

La trama de protocolo empieza con un preámbulo, que es un patrón alternativo de unos y ceros. La longitud del preámbulo es siete bytes. El preámbulo está seguido por un delimitador de trama de inicio (SFD – Start of Frame, en inglés). El delimitador de trama de inicio tiene una longitud de un byte e incluye un patrón alternativo de unos y ceros, que finaliza con dos unos consecutivos. El delimitador de trama de inicio está seguido por seis bytes que definen una dirección de MAC de destino (DA – Destination Address, en inglés) de la trama de protocolo y por seis bytes que definen una dirección de MAC de fuente (SA – Source Address, en inglés) de la trama de protocolo. El siguiente campo incluye una identificación de protocolo de marcado (TPID – Tagging Protocol IDentification, en inglés). Un valor hexadecimal de 8100 indica el protocolo 802.1 q/p del IEEE. El siguiente campo incluye información de control de marca (TCI – Tag Control Information, en inglés). Como se ilustra en la parte inferior de la Figura 6, la información de control de marca incluye tres bits de prioridad, seguidos por un bit definido como indicador de formato canónico (CFI – Canonical Format Indicator, en inglés) y doce bits de una identificación de red de área local virtual (VLAN ID – Virtual Local Area Network Identification, en inglés). El campo TCI puede denominarse asimismo marca de VLAN. El campo TCI está seguido por un campo de Longitud de tipo, de dos bytes de longitud. Este campo indica el número de bytes de datos del cliente MAC contenidos en el campo de datos de la trama de protocolo o la identificación del tipo de trama si la trama es ensamblada utilizando un formato opcional. El campo Longitud de tipo está seguido por el campo de datos, que puede ser una secuencia de 48 a 1500 bytes de longitud. El campo de datos está seguido por un valor de comprobación de redundancia cíclica (CRC – Cyclic Redundancy Check, en inglés), que es generado por el dispositivo fuente de MAC y es utilizado por el dispositivo de destino de MAC para comprobar la integridad de las tramas de protocolo recibidas.

En el campo de TCI, los bits de prioridad definen una prioridad de usuario. Detalles relativos al mapeo de los ajustes de los bits de prioridad a las prioridades del usuario se definen en el estándar 802.1 p del IEEE. El bit CFI se utiliza para proporcionar compatibilidad con las redes tanto del tipo de Ethernet como de Anillo (Token Ring, en inglés). El ID de VLAN se utiliza para distinguir entre diferentes redes de área local virtual (VLAN).

De acuerdo con los conceptos descritos en esta memoria, la información en los paquetes de datos de DL se utiliza en el dispositivo de comunicación 100 para generar localmente reglas de clasificación de paquetes para paquetes de datos de UL. En esta memoria, debe observarse que en muchos escenarios prácticos, un flujo de paquetes de datos de IP es típicamente bidireccional. Incluso si el transporte de los datos de carga útil se produce solo en una dirección, por ejemplo sobre la base de los paquetes de TCP, el flujo de paquetes de IP incluirá también típicamente paquetes de control, por ejemplo paquetes de acuse de recibo de TCP, transmitidos en la dirección opuesta. Además, las direcciones de IP de fuente y de destino y los números de puerto de un flujo de paquetes de IP son típicamente simétricas, es decir, el punto final de destino (identificado por una dirección de IP y un numero de puerto) en una dirección es el mismo que el punto final de fuente (identificado por una dirección de IP y un número de puerto) en la otra dirección, y viceversa. Debido a la simetría, paquetes que fluyen en sentidos opuestos del mismo flujo que el paquete de IP tendrán identificadores de dirección “complementarios” e identificadores de puerto “complementarios”, lo que significa que el identificador de fuente en una dirección es el mismo que el identificador de destino en la otra dirección.

De acuerdo con los conceptos explicados en lo que sigue, se asumirá que el tráfico de datos de DL es de alguna manera asignado a las clases de tráfico 50 y provistos de un marcado correspondiente. Esto puede efectuarse mediante el clasificador de tráfico 210 del nodo de puerta de enlace de red 220. En el ejemplo ilustrado, el nodo de control 300 señala las reglas de clasificación de paquetes de DL 215 al nodo de puerta de enlace de red 220. No obstante, puede utilizarse también otra manera de proporcionar las reglas de clasificación de paquetes de DL 215 al nodo de puerta de enlace de red 220. Utilizando las reglas de clasificación de paquetes de DL 215, el clasificador de tráfico 220 en el nodo de puerta de enlace de red 220 asigna los paquetes de DL a las clases de tráfico 50 y marca los paquetes de datos de DL de acuerdo con esto. Este marcado puede ser efectuado ajustando el campo de DSCP en la cabecera de los paquetes de datos, ajustando los bits de prioridad de los paquetes de datos y/o proporcionando a los paquetes de datos una marca de VLAN. Además, si los paquetes de datos salientes van a ser transmitidos utilizando protocolo de tunelación, este marcado de los paquetes de datos salientes puede conseguirse también proporcionando a los paquetes de datos una identificación de túnel.

Como se ha explicado anteriormente, el dispositivo de comunicación 100 incluye el clasificador de tráfico 110 que opera sobre la base de las reglas de clasificación de paquetes de UL 115 y que soporta un modo reflexivo de generar las reglas de clasificación de paquetes de UL. En el modo reflexivo, el clasificador de tráfico 110 está configurado para detectar los paquetes de datos salientes que incluyen un segundo identificador que es complementario con respecto al primer identificador. En el segundo identificador complementario, un elemento de punto final de destino, por ejemplo, una dirección de IP de destino y/o un puerto de destino, es el mismo que un elemento de punto final de fuente, por ejemplo, la dirección de IP de fuente y/o el puerto de fuente, en el primer identificador. Cada uno de los identificadores primero y segundo puede ser una tupla de orden 5 de IP. Monitorizando los paquetes de datos de DL recibidos, el clasificador de tráfico 110 genera las reglas de clasificación de paquetes de UL 115 de tal manera que los paquetes de datos salientes que tienen el segundo identificador complementario son asignados a la misma clase de tráfico 50 que los paquetes de datos entrantes que tienen el primer identificador. De esta manera, no se requiere señalar explícitamente las reglas de clasificación de paquetes de UL 115 al dispositivo de comunicación 100. Por otro lado, las reglas de clasificación de paquetes de UL 115 pueden ser adaptadas flexiblemente a escenarios de comunicación específicos, que pueden ser controlados por el operador de la red mediante la clasificación de tráfico de DL.

En el modo reflexivo, si el clasificador de tráfico 110 detecta un nuevo paquete de datos de IP con paquetes de datos entrantes en la dirección de DL, puede generar automáticamente una regla de clasificación de paquetes de UL 115 correspondiente. Si los paquetes de datos entrantes del flujo de paquetes de IP contienen cada uno una tupla de orden 5 de IP, la regla de clasificación de paquetes de UL 115 estará configurada para asignar paquetes de datos salientes que contienen una tupla de orden 5 de IP complementaria a la misma clase de tráfico 50 que se reciben los paquetes de datos entrantes. Además, los paquetes de datos de UL son marcados de acuerdo con su clasificación, por ejemplo utilizando el mismo marcado que en los paquetes de datos de DL de esta clase de tráfico. Este marcado puede conseguirse ajustando el campo de DSCP en la cabecera de los paquetes de datos, proporcionando a los paquetes de datos una marca de VLAN, y/o ajustando los bits de prioridad de los paquetes de datos. Además, si los paquetes de datos salientes van a ser transmitidos utilizando un protocolo de tunelación, este marcado de los paquetes de datos salientes puede conseguirse también proporcionando a los paquetes de datos una identificación de túnel.

La estructura de un identificador y de un identificador complementario, que están basados en la tupla de orden 5 de IP, se ilustra en la Figura 7. No obstante, debe entenderse que también son posibles otros tipos de identificadores y de identificadores complementarios. En general, en el identificador complementario al menos un elemento del identificador reaparece como otro elemento. Por ejemplo, en el identificador complementario del paquete de datos saliente, el elemento de fuente del identificador en el paquete de datos entrante puede reaparecer como elemento de destino. De acuerdo con una realización, el identificador incluye una dirección de fuente y una dirección de destino y el identificador complementario incluye una dirección de fuente correspondiente a la dirección de destino del identificador, y una dirección de destino correspondiente a la dirección de fuente del identificador.

Como se muestra en la Figura 7, un identificador sobre la base de la tupla de orden 5 de IP puede incluir una dirección de fuente A, una dirección de destino B, un puerto de fuente C, un puerto de destino D y un identificador de

protocolo X. El identificador complementario correspondiente tendrá entonces una dirección de fuente B, una dirección de destino A, un puerto de fuente D, un puerto de destino C y un identificador de protocolo X. En otras palabras, en el identificador complementario la dirección de fuente y la dirección de destino están intercambiadas en comparación con el identificador. De manera similar, en el identificador complementario el puerto de fuente y el puerto de destino están intercambiados en comparación con el identificador. El identificador de protocolo permanece igual. En otras realizaciones, pueden utilizarse diferentes tipos de identificador y de identificador complementario, por ejemplo, sobre la base solo de una parte de la tupla de orden 5 de IP. Por ejemplo, en el identificador complementario, solo la dirección de fuente y la dirección de destino podrían estar intercambiadas en comparación con el identificador.

En lo que sigue, se explicará con más detalle un proceso de manejo de paquetes de datos de UL de acuerdo con una realización de la invención, por referencia a las estructuras mostradas en la Figura 1.

Inicialmente, los paquetes de datos de UL, por ejemplo, los paquetes de datos relativos a un servicio específico tal como un servicio de voz sobre IP, pueden ser transmitidos desde el dispositivo de comunicación 100 hasta la puerta de enlace de red 220 mientras son asignados a una clase de tráfico por defecto de entre las clases de tráfico 50, por ejemplo, la clase de tráfico de internet. El flujo de paquetes de IP correspondiente incluirá entonces también los paquetes de datos transmitidos en la dirección de DL, por ejemplo, paquetes de acuse de recibo. Utilizando las reglas de clasificación de paquetes de DL 215, el clasificador de tráfico 210 en el nodo de puerta de enlace de red 220 asignará estos paquetes de datos de DL a una clase de tráfico deseada, por ejemplo, tráfico de voz, y efectuará un correspondiente marcado de los paquetes de datos de DL. Como se ha mencionado anteriormente, este marcado puede implicar ajustar el campo de DSCP en la cabecera de los paquetes de datos de DL, proporcionando a los paquetes de datos de DL una marca de VLAN, proporcionando a los paquetes de datos de DL una identificación de túnel, y/o ajustando los bits de prioridad de los paquetes de datos de DL.

En el modo reflexivo, el clasificador de tráfico 110 en el dispositivo de comunicación 100 detecta entonces los paquetes de datos de DL entrantes y genera una regla de clasificación de paquetes de UL 115, que opera sobre la base de una tupla de orden 5 de IP que es complementaria de una tupla de orden 5 de IP en los paquetes de datos entrantes recibidos. En esta memoria, debe entenderse que diferentes flujos de paquetes de IP pueden tener la misma clase de tráfico 50 y que pueden utilizarse múltiples reglas de clasificación de paquetes de UL 115 para asignar paquetes de datos de UL salientes a una clase de tráfico 50.

Además del modo reflexivo de generar las reglas de clasificación de paquetes de UL 115, el clasificador de tráfico 110 puede estar provisto también de otros modos de clasificación, por ejemplo, que operan sobre la base de las reglas de clasificación de paquetes de UL señaladas desde la red, que operan sobre la base de las reglas de clasificación de paquetes de UL configuradas estadísticamente, o que operan sobre la base del mapeo de puertos. El modo reflexivo puede ser activado en respuesta a la recepción de una señal de control desde la red, por ejemplo, cuando se inicializa la conexión entre el dispositivo de comunicación 100 y el nodo de puerta de enlace de red 220 o en un procedimiento de actualización.

El dispositivo de comunicación 100 puede ser provisto también de una funcionalidad para indicar a la red de comunicación que soporta el modo reflexivo descrito anteriormente de generar las reglas de clasificación de paquetes de UL 115. Por ejemplo, esto podría estar incluido en la inicialización de la conexión entre el dispositivo de comunicación 100 y el nodo de puerta de enlace de red 220. A modo de ejemplo, podría añadirse un elemento de información a la señalización utilizada durante la inicialización de la conexión. Por medio de este elemento de información, el dispositivo de comunicación 100 puede indicar que soporta el modo reflexivo. Y la red puede señalar al dispositivo de comunicación 100 si debe utilizarse el modo reflexivo.

En algunas realizaciones, la información de que el dispositivo de comunicación 100 soporta el modo reflexivo de generar las reglas de clasificación de UL 115 puede ser también distribuida entre nodos de red, por ejemplo, al nodo de control 300.

De acuerdo con algunas realizaciones, el modo reflexivo de generar reglas de clasificación de UL 115 puede ser activado selectivamente para un subgrupo de las clases de tráfico 50, por ejemplo, solo para una clase de tráfico. Por ejemplo, el modo reflexivo podría ser activado solo para tráfico de voz y/o tráfico multimedia. Esto puede resultar útil si no todas las aplicaciones o servicios requieren la activación del modo reflexivo. Por ejemplo, en algunos casos la tupla de orden 5 de IP en los paquetes de datos de un servicio puede ser definida estadísticamente y puede utilizarse una regla de clasificación de paquetes de UL 115 estática correspondiente en el dispositivo de comunicación 100. Asimismo, el mapeo de puertos podría ser utilizado para algunas de las clases de tráfico 50, mientras que la clasificación de tráfico a una o más de otras clases de tráfico se efectúa en el modo reflexivo.

En algunas realizaciones, la red puede señalar al dispositivo de comunicación 100 si el modo reflexivo de generación de las reglas de clasificación de UL 115 debe ser aplicado o no, por ejemplo, utilizando una señalización correspondiente en el enlace entre el nodo de puerta de enlace de red 220 y el dispositivo de comunicación 100. En tales casos, la señalización del dispositivo de comunicación 100 a la red de comunicación de que el modo reflexivo está soportado podría ser implementada también por cada clase de tráfico. Es decir, la señalización correspondiente

podría especificar el soporte del modo reflexivo para una cierta clase de tráfico o grupo de clases de tráfico, por ejemplo, el tráfico de voz y el tráfico multimedia.

La Figura 8 ilustra además una implementación de ejemplo del dispositivo de comunicación 100. Como se ha explicado anteriormente, el dispositivo de comunicación puede ser un terminal móvil, por ejemplo, el UE 40 explicado en conexión con la Figura 1, o una puerta de enlace residencial, por ejemplo, la RG 35 explicada en conexión con la Figura 1.

De acuerdo con la implementación ilustrada, el dispositivo de comunicación 100 incluye al menos una primera interfaz 130 para el acoplamiento al nodo de puerta de enlace de red 220 a través del nodo de acceso fijo 250. La interfaz 130 es implementada como una interfaz bidireccional, es decir, incluye una interfaz de recepción (RX) para la recepción de paquetes de datos de DL y una interfaz de transmisión (TX) para la transmisión de paquetes de datos de UL. En algunas realizaciones, por ejemplo, si el dispositivo de comunicación es implementado como una puerta de enlace residencial, puede también incluir al menos una segunda interfaz 140 para el acoplamiento a otros dispositivos, por ejemplo, a los dispositivos de casa del abonado como se ilustra en la Figura 1. La segunda interfaz 140 puede ser implementada también como una interfaz bidireccional, es decir, incluir una interfaz de recepción (RX) y una interfaz de transmisión (TX). Además, el dispositivo de comunicación 100 incluye un procesador 150 acoplado a la interfaz o a las interfaces 130, 140 y una memoria 160 acoplada al procesador 150. La memoria 160 puede incluir una memoria de solo lectura (ROM – Read Only Memory, en inglés), por ejemplo, una ROM rápida, una memoria de acceso aleatorio (RAM – Random Access Memory, en inglés), por ejemplo una RAM dinámica (DRAM – Dynamic RAM, en inglés) o una RAM estática (SRAM – Static RAM, en inglés), un almacenamiento masivo, por ejemplo un disco duro o un disco de estado sólido, u otros. La memoria 160 incluye código de programa configurado adecuadamente para ser ejecutado por el procesador 150 para implementar las funcionalidades descritas anteriormente del dispositivo de comunicación 100. Más específicamente, la memoria 160 puede incluir un módulo generador de reglas 170 configurado para implementar el modo reflexivo de generación de reglas de clasificación de paquetes de UL y un módulo de clasificación de tráfico 180 configurado para clasificar los paquetes de datos de UL salientes en la manera descrita anteriormente aplicando las reglas de clasificación de paquetes de UL, y para marcar los paquetes de datos de UL salientes de acuerdo con esto. De acuerdo con esto, el clasificador de tráfico 110 puede ser implementado haciendo que el procesador 150 ejecute el módulo generador de reglas 170 y el módulo de clasificación de tráfico 180.

Debe entenderse que la estructura ilustrada en la Figura 8 es meramente esquemática y que el dispositivo de comunicación 100 puede incluir de hecho otros componentes que, en aras de la claridad, no han sido ilustrados. Asimismo, debe entenderse que la memoria 160 puede incluir otros tipos de módulos de código de programa, que no han sido ilustrados, por ejemplo módulos de código de programa para la implementación de funcionalidades conocidas de un terminal móvil o de una puerta de enlace residencial.

La Figura 9 muestra un diagrama de flujo que ilustra un método 900 para manejar el tráfico de datos de UL, que puede ser utilizado para implementar los conceptos mencionados anteriormente. El método puede ser implementado en un dispositivo de comunicación que tenga acceso a una red de comunicación a través de un acceso fijo, por ejemplo, en el UE 40 o en la RG 35 de la Figura 1.

En la etapa 910, los paquetes de datos entrantes con un primer identificador son recibidos en el dispositivo de comunicación. Los paquetes de datos son recibidos a través del acceso fijo. Para ello, el dispositivo de comunicación puede ser acoplado al acceso fijo a través de un nodo de acceso fijo intermedio. Los paquetes de datos son identificados por un primer identificador, por ejemplo, una tupla de orden 5 de IP o por otro identificador que incluya un identificador de dirección de destino y un identificador de dirección de fuente. Además, los paquetes de datos entrantes son asociados con una clase de tráfico, por ejemplo, mediante un marcado proporcionado en los paquetes de datos.

En la etapa 920, se detectan paquetes de datos salientes con un segundo identificador complementario.

En la etapa 930, paquetes de datos salientes con un segundo identificador son asignados a la misma clase de tráfico que los paquetes de datos entrantes con el primer identificador.

La detección de paquetes de datos salientes en la etapa 920 y la asignación a la misma clase de tráfico en la etapa 930 pueden efectuarse sobre la base de una regla de clasificación de paquetes. La regla de clasificación de paquetes puede ser generada en el dispositivo de comunicación monitorizando los paquetes de datos entrantes recibidos.

A continuación, en la etapa 940 opcional, los paquetes de datos salientes pueden ser provistos de un marcado que indica la clase de tráfico a la cual han sido asignados los paquetes de datos salientes. Este marcado puede efectuarse ajustando un DSCP de los paquetes de datos salientes, ajustando bits de prioridad de los paquetes de datos salientes y/o que incluyen una marca de VLAN o una identificación de túnel en los paquetes de datos salientes. Los bits de prioridad pueden ser parte de la marca de VLAN.

De acuerdo con los conceptos explicados anteriormente, la asignación dinámica de tráfico de datos saliente desde un dispositivo de comunicación a una clase de tráfico deseada es posible sin requerir una señalización compleja

hacia el dispositivo de comunicación. La asignación puede ser adaptada de acuerdo con las condiciones de operación o sobre la base de datos de políticas, por ejemplo, sobre la base de datos de políticas específicas para un usuario y/o, si el tráfico de datos salientes se refiere a un servicio específico, sobre la base de políticas específicas para un servicio. Además, la asignación podría ser dependiente de la hora del día, del día de la semana o de otros parámetros. Una variedad de políticas diferentes puede ser así definida para controlar la asignación del tráfico de datos a una clase de tráfico. Una de tales políticas puede incluso ser bloquear tráfico de datos relativos a un servicio específico.

Debe entenderse que los conceptos explicados anteriormente son meramente de ejemplo y susceptibles de varias modificaciones. Por ejemplo, los nodos de red como se ilustran en las Figs. 1 y 2 no necesitan ser implementados como nodos separados, sino que dos o más nodos pueden ser integrados en un único componente. Los conceptos pueden ser aplicados en varios tipos de redes de comunicación y en varios tipos de dispositivos de comunicación. Además o como alternativa a las tuplas de orden 5 de IP, pueden utilizarse otros identificadores e identificadores complementarios, así como para implementar los conceptos. Los conceptos pueden ser implementados mediante hardware dedicado y/o mediante software para ser ejecutado mediante un procesador de múltiples propósitos en uno de los nodos implicados.

REIVINDICACIONES

1. Método de manejo del tráfico de red en un dispositivo de comunicación (100), que comprende:

- recibir paquetes de datos de enlace descendente entrantes a través de un acceso fijo en el dispositivo de comunicación (100), incluyendo los paquetes de datos de enlace descendente entrantes un primer identificador y estando marcados de acuerdo con una clase de tráfico (50) a la que se han asignado, incluyendo dicho primer identificador una dirección de fuente;

- detectar paquetes de datos de enlace ascendente salientes para ser transmitidos a través de un acceso fijo desde el dispositivo de comunicación (100), incluyendo los citados paquetes de datos de enlace ascendente salientes un segundo identificador, incluyendo el citado segundo identificador una dirección de destino que es igual a la dirección de fuente del citado primer identificador; y

- marcar los paquetes de datos de enlace ascendente salientes detectados que tienen el citado segundo identificador de acuerdo con la misma clase de tráfico (50) que los paquetes de datos de enlace descendente entrantes que tienen el citado primer identificador.

2. El método de acuerdo con la reivindicación 1,

en el que los paquetes de datos de enlace descendente entrantes y los paquetes de datos de enlace ascendente salientes se realizan como paquetes de datos IP, en donde el primer identificador y el segundo identificador se realizan como una tupla de orden 5 de IP del paquete de datos IP respectivo, en donde la tupla de orden 5 de IP incluye una dirección de fuente, una dirección de destino, un puerto de fuente, un puerto de destino y un identificador de protocolo.

3. El método de acuerdo con la reivindicación 2,

en el que el segundo identificador incluye una dirección IP de destino y/o puerto de destino, que son lo mismo que una dirección IP de fuente y/o puerto de fuente en el primer identificador.

4. El método de acuerdo con una cualquiera de las reivindicaciones precedentes,

en el que en el segundo identificador, la dirección de fuente y la dirección de destino están intercambiadas en comparación con el primer intercambiador y/o en el que en el segundo identificador el puerto de fuente y el puerto de destino están intercambiados en comparación con el primer identificador.

5. El método de acuerdo con una cualquiera de las reivindicaciones precedentes, que comprende:

- monitorizar los paquetes de datos de enlace descendente entrantes recibidos; y

- generar una regla de clasificación de paquetes para marcar los paquetes de datos de enlace ascendente salientes a la misma clase de tráfico (50) sobre la base de los paquetes de datos de enlace descendente entrantes monitorizados.

6. El método de acuerdo con una cualquiera de las reivindicaciones precedentes,

en el que el citado marcado de paquetes de datos de enlace ascendente salientes a la misma clase de tráfico (50) se activa sobre la base de una señal de control.

7. El método de acuerdo con una cualquiera de las reivindicaciones precedentes,

en el que el citado marcado de los paquetes de datos de enlace ascendente salientes se activa selectivamente para un subgrupo de clases de tráfico (50) múltiples.

8. El método de acuerdo con una cualquiera de las reivindicaciones precedentes,

en el que el citado marcado de los paquetes de datos de enlace descendente entrantes es un campo ajustado de Punto de código de servicios diferenciados de los paquetes de datos, bits de prioridad ajustados de los paquetes de datos, una marca de red de área local virtual proporcionada con los paquetes de datos y/o un identificador de túnel proporcionado con los paquetes de datos.

9. El método de acuerdo con una cualquiera de las reivindicaciones precedentes,

en el que el citado marcado de los paquetes de datos de enlace ascendente salientes comprende ajustar un campo de Punto de código de servicios diferenciados de los paquetes de datos, ajustando los bits de prioridad de los paquetes de datos, proporcionando a los paquetes de datos una marca de red de área local virtual y/o proporcionando a los paquetes de datos un identificador de túnel.

10. El método de acuerdo con una cualquiera de las reivindicaciones precedentes, que comprende:

- indicar a un componente de red (220) que el citado dispositivo de comunicación (100) es capaz del citado marcado de paquetes de datos de enlace ascendente salientes a la misma clase de tráfico (50).

11. Un dispositivo de comunicación (100), que comprende:

- una interfaz (120) configurada para recibir paquetes de datos de enlace descendente entrantes a través de un acceso fijo desde una red, en donde los paquetes de datos de enlace descendente entrantes son marcados de acuerdo con una clase de tráfico (50) a la que están asignados;

- una interfaz (120) configurada para enviar paquetes de datos de enlace ascendente salientes a través de un acceso fijo a la red;

- un clasificador de tráfico (110) configurado para detectar paquetes de datos de enlace descendente entrantes que incluyen un primer identificador y paquetes de datos de enlace ascendente salientes que incluyen un segundo identificador, incluyendo el citado primer identificador una dirección de fuente e incluyendo el citado segundo identificador una dirección de destino que es igual a la dirección de fuente del citado primer identificador, y estando el clasificador de tráfico (110) configurado para marcar a los citados paquetes de datos de enlace ascendente salientes que tienen citado segundo identificador a la misma clase de tráfico (50) que los paquetes de datos de enlace descendente entrantes que tienen el primer identificador.

12. El dispositivo de comunicación (100) de acuerdo con la reivindicación 11, en el que el dispositivo de comunicación (100) está configurado para ser operado de acuerdo con el método de acuerdo con una cualquiera de las reivindicaciones 1 a 10.

13. Un producto de programa informático, que comprende código de programa que, cuando es ejecutado por un procesador de un dispositivo de comunicación (100) hace que el dispositivo de comunicación (100) opere de acuerdo con un método de acuerdo con una cualquiera de las reivindicaciones 1 a 10.

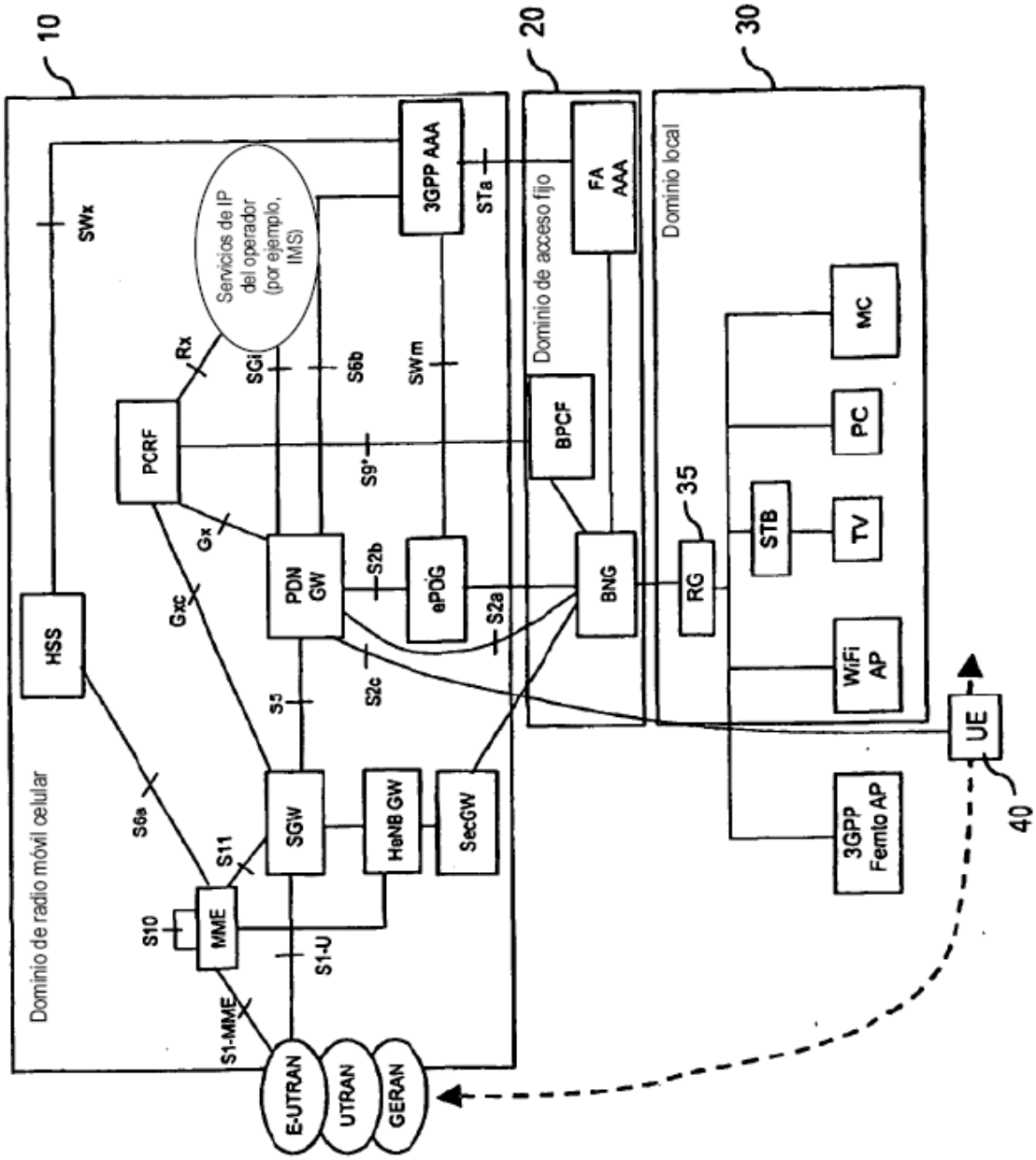
10
20
30
Dominio de radio móvil celular
Dominio de acceso fijo
Dominio local
SWx
Servicios de IP del operador (por ejemplo, IMS)
3GPP AAA
STa
FA AAA
Rx
SGi
S6b
SWm
PCRF
BPCF
S9'
MC
PC
STB
TV
35
Gx
Gxc
PDN GW
S2b
ePDG
S2a
BNG
RG
HSS
S5
S2c
WiFi AP
UE
S6a
S11
SGW
HeNB GW
SecGW
3GPP Femto AP
40
S10
MME
S1-U
S1-MME
E-UTRAN
UTRAN
GERAN

FIG. 1

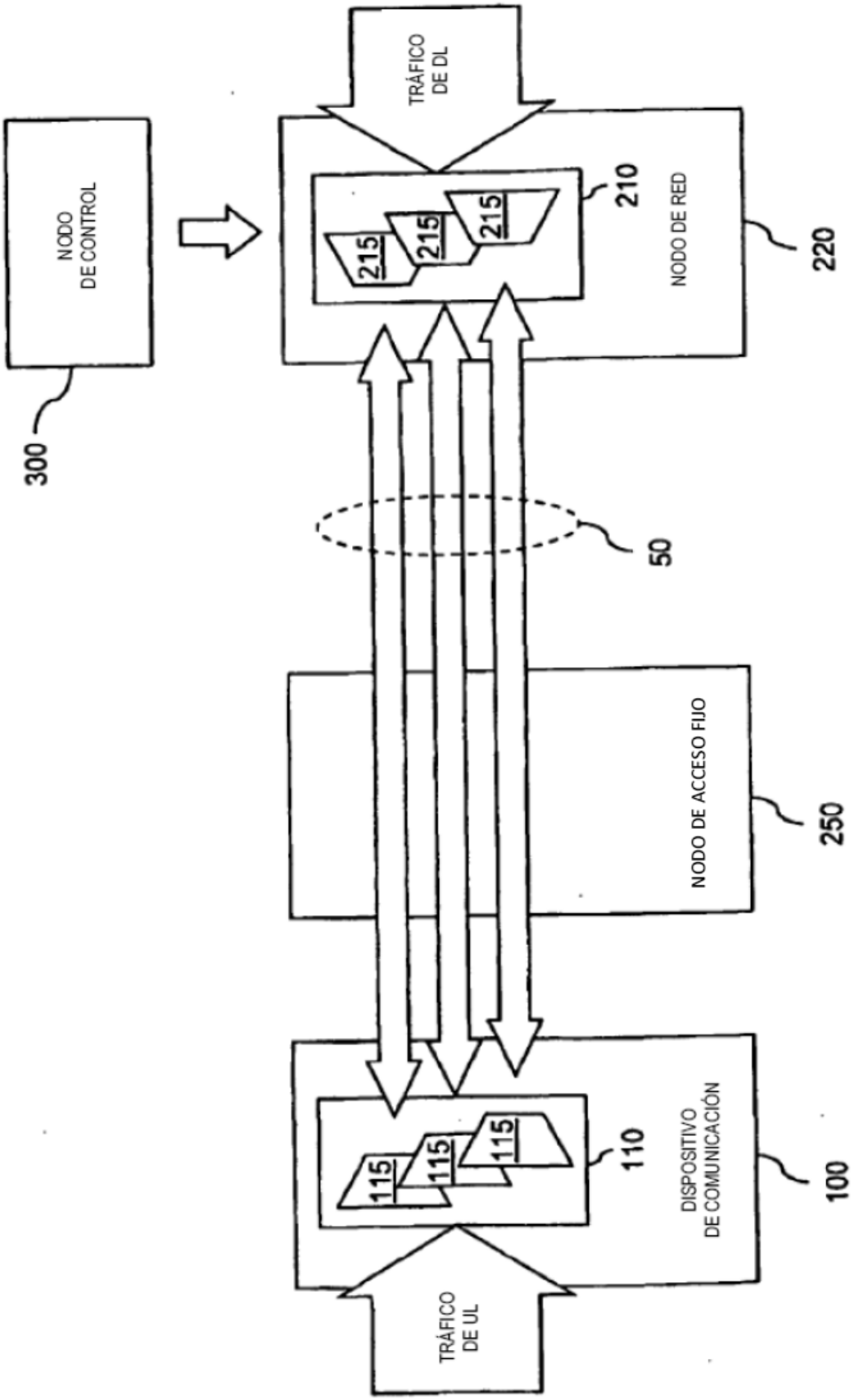
NODO DE CONTROL
300
TRÁFICO DE DL
210
215
215
215
NODO DE RED
220
50
NODO DE ACCESO FIJO
250
DISPOSITIVO DE COMUNICACIÓN
100
110
115
115
115
TRÁFICO DE UL

FIG. 2

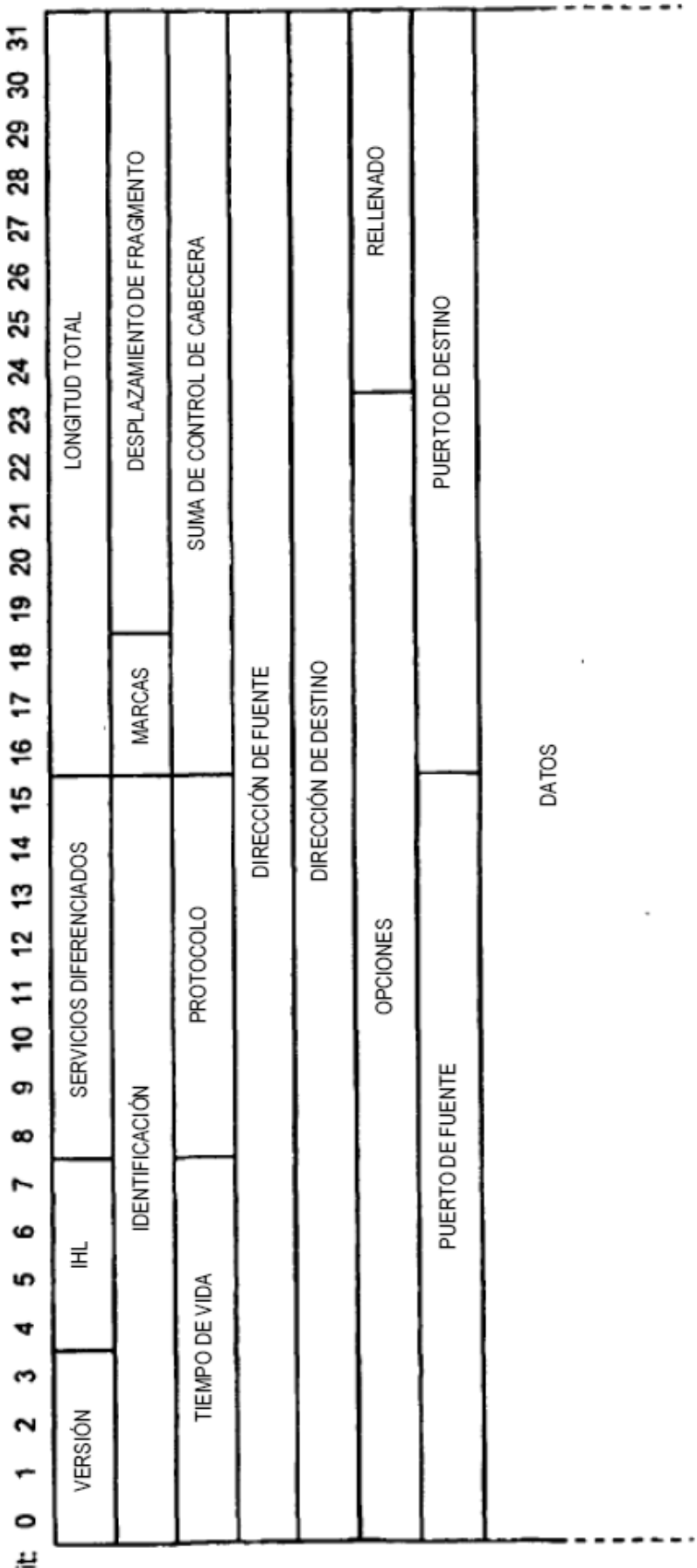
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSIÓN
IHL
SERVICIOS DIFERENCIADOS
LONGITUD TOTAL
IDENTIFICACIÓN
MARCAS
DESPLAZAMIENTO DE FRAGMENTO
TIEMPO DE VIDA
PROTOCOLO
SUMA DE CONTROL DE CABECERA
DIRECCIÓN DE FUENTE
DIRECCIÓN DE DESTINO
OPCIONES
RELLENADO
PUERTO DE FUENTE
PUERTO DE DESTINO
DATOS

FIG. 3

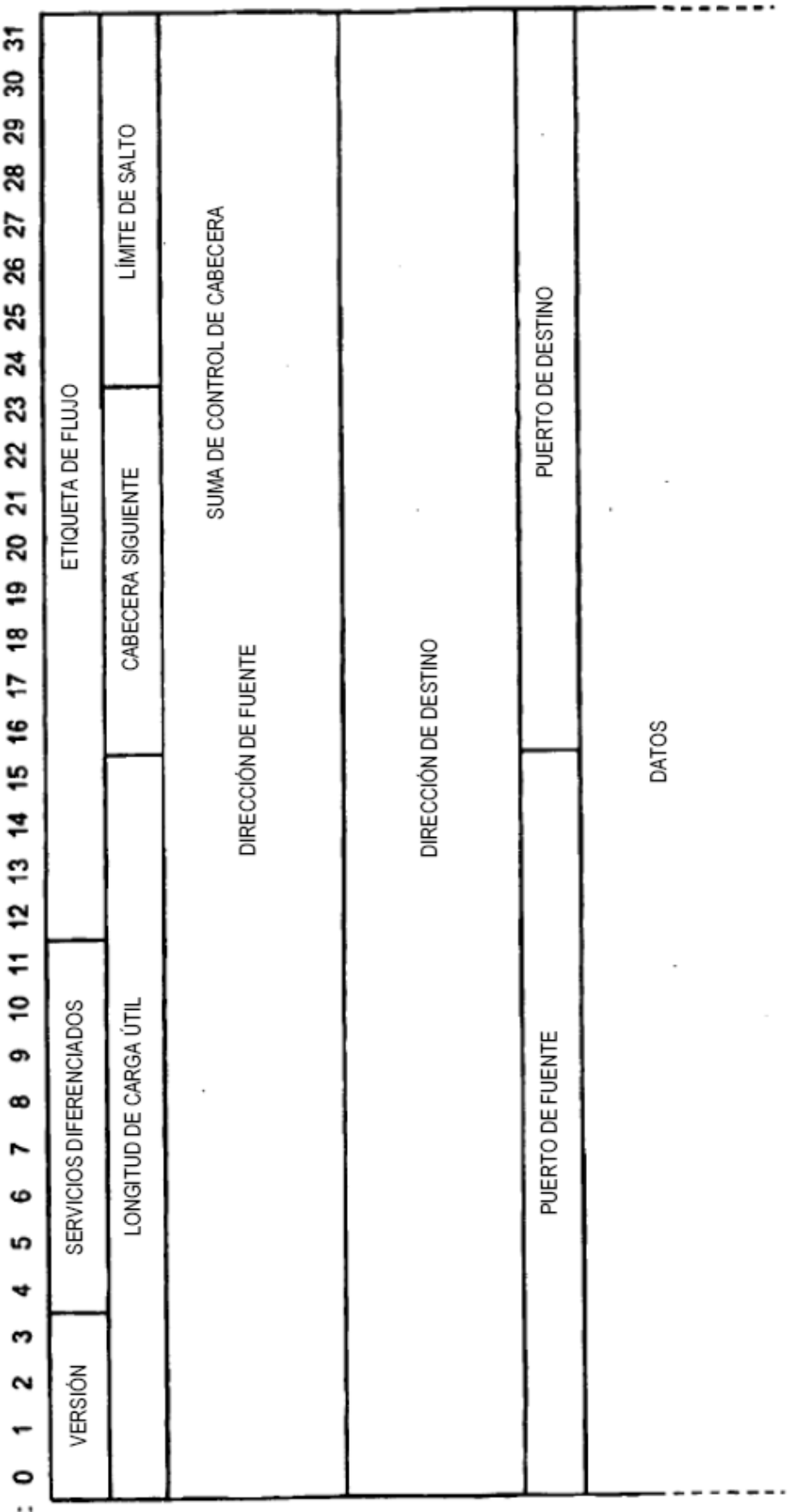
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSIÓN
SERVICIOS DIFERENCIADOS
ETIQUETA DE FLUJO
LONGITUD DE CARGA ÚTIL
CABECERA SIGUIENTE
LÍMITE DE SALTO
DIRECCIÓN DE FUENTE
SUMA DE CONTROL DE CABECERA
DIRECCIÓN DE DESTINO
PUERTO DE FUENTE
PUERTO DE DESTINO
DATOS

FIG. 4

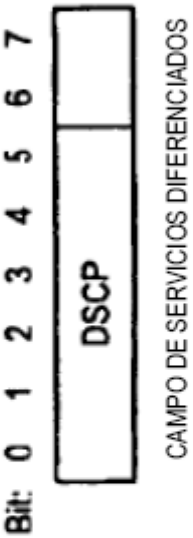

FIG. 5

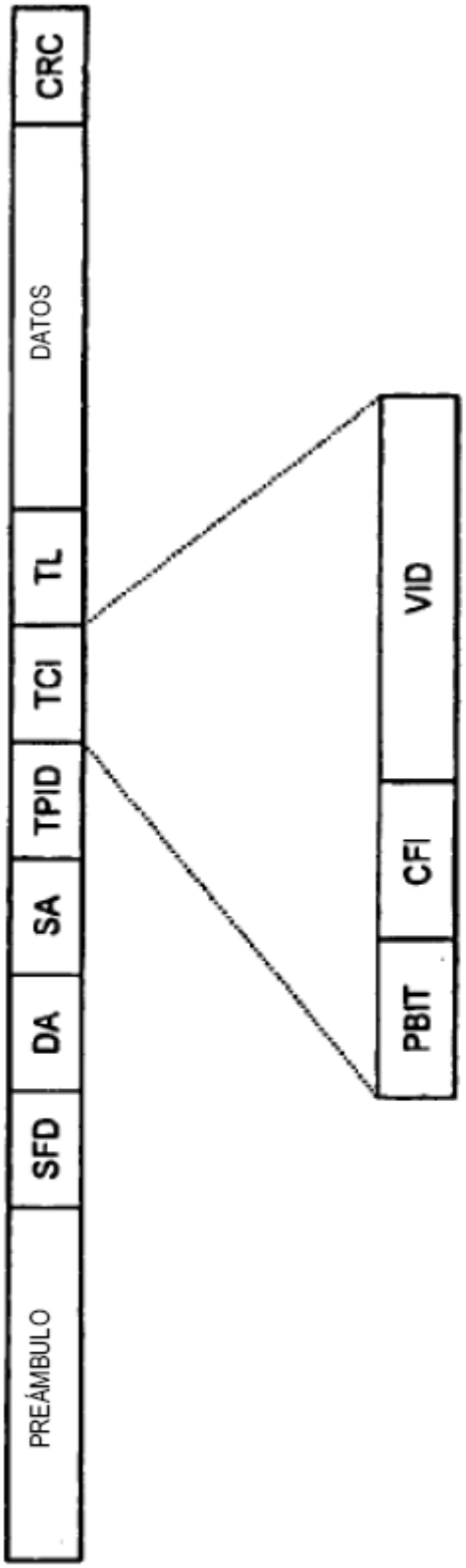

FIG. 6

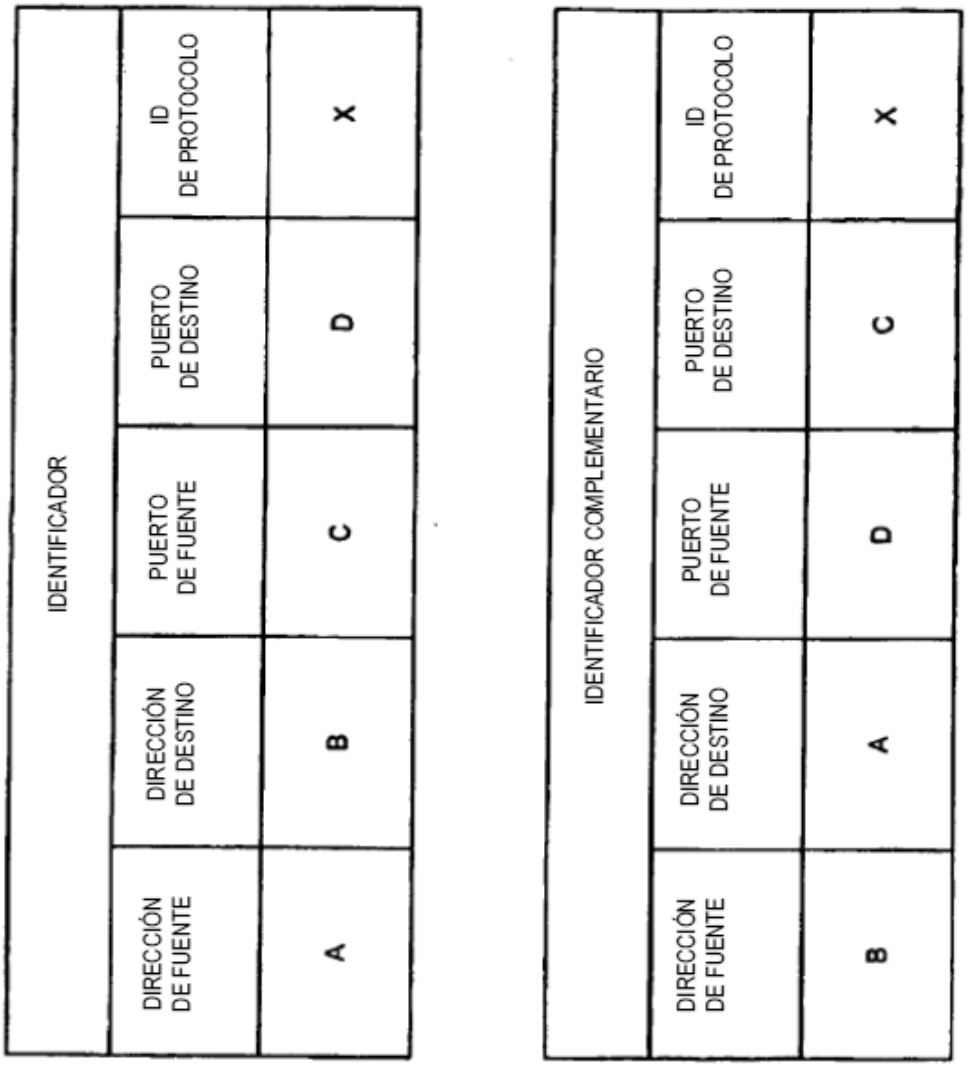
IDENTIFICADOR
DIRECCIÓN DE FUENTE
DIRECCIÓN DE DESTINO
PUERTO DE FUENTE
PUERTO DE DESTINO
ID DE PROTOCOLO
A
B
C
D
X
IDENTIFICADOR COMPLEMENTARIO
DIRECCIÓN DE FUENTE
DIRECCIÓN DE DESTINO
PUERTO DE FUENTE
PUERTO DE DESTINO
ID DE PROTOCOLO
B
A
D
C
X

FIG. 7

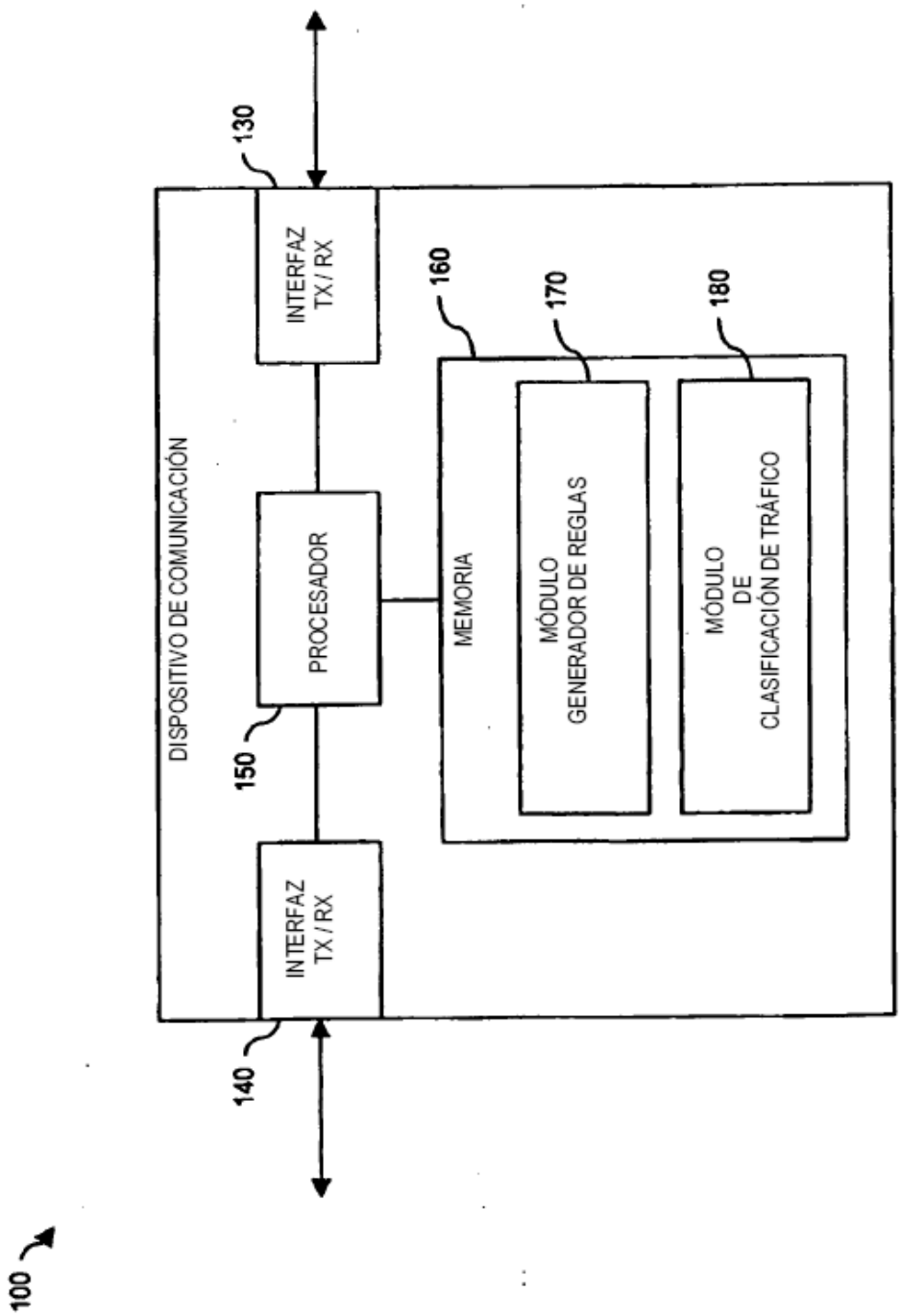
100
DISPOSITIVO DE COMUNICACIÓN
130
INTERFAZ TX / RX
150
PROCESADOR
140
INTERFAZ TX / RX
160
MEMORIA
170
MÓDULO GENERADOR DE REGLAS
180
MÓDULO DE CLASIFICACIÓN DE TRÁFICO

FIG. 8

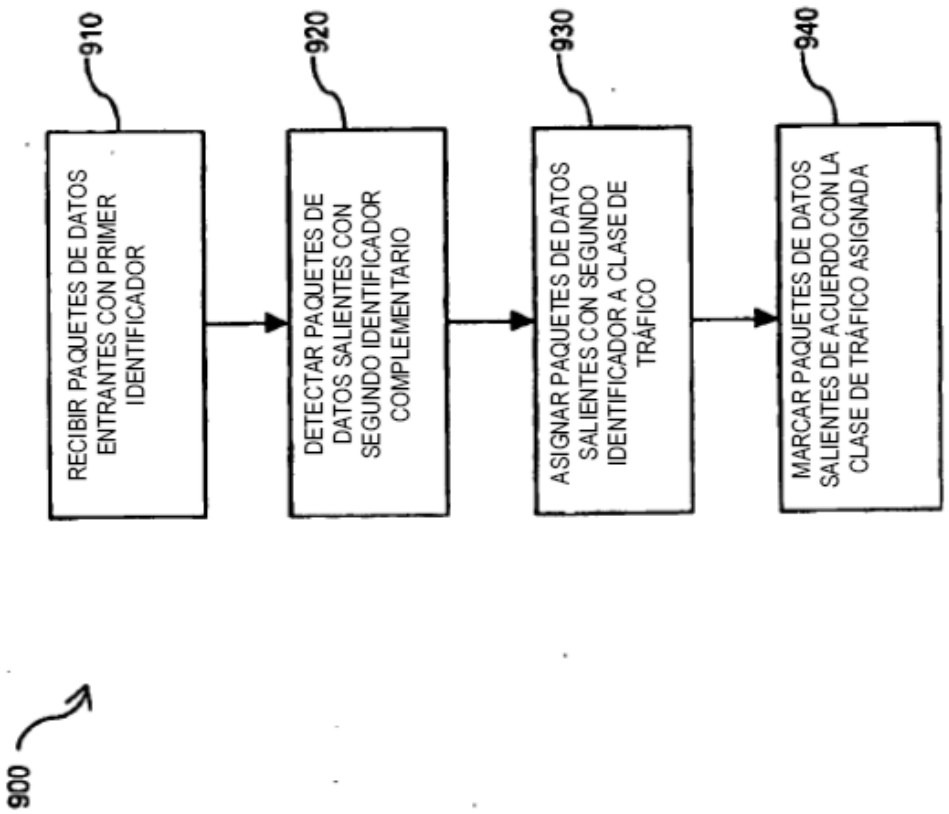
900
910
RECIBIR PAQUETES DE DATOS ENTRANTES CON PRIMER IDENTIFICADOR
920
DETECTAR PAQUETES DE DATOS SALIENTES CON SEGUNDO IDENTIFICADOR COMPLEMENTARIO
930
ASIGNAR PAQUETES DE DATOS SALIENTES CON SEGUNDO IDENTIFICADOR A CLASE DE TRÁFICO
940
MARCAR PAQUETES DE DATOS SALIENTES DE ACUERDO CON LA CLASE DE TRÁFICO ASIGNADA

FIG. 9