(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 567 558**

(51) Int. CI.:

H04W 28/18 (2009.01)
H04W 72/12 (2009.01)
H04L 12/70 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.04.2009 E 14170345 (4)**

(97) Fecha y número de publicación de la concesión europea: **03.02.2016 EP 2773147**

(54) Título: **Técnicas para gestionar tráfico de red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.04.2016

(73) Titular/es:

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

(72) Inventor/es:

LUDWIG, REINER y
EKSTRÖM, HANNES

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Técnicas para gestionar tráfico de red

Sector técnico

La presente invención se refiere a técnicas para gestionar tráfico de red

Antecedentes

En las redes de comunicación móvil es conocido el dirigir tráfico de red relacionado con un servicio específico a una portadora con una cierta calidad de servicio (QoS, quality of service). A este respecto, se considera que una portadora es un trayecto o contexto de transmisión de información, de características definidas, por ejemplo la capacidad, el retardo y/o la tasa de bits erróneos. Habitualmente, se establecerán una serie de portadoras entre una pasarela de una red de comunicación móvil y un equipo de usuario, por ejemplo un teléfono móvil u otro tipo de terminal móvil. Una portadora puede transportar tráfico de datos de enlace descendente (DL) en el sentido de la red al equipo de usuario, y puede transportar tráfico de datos en el sentido del enlace ascendente (UL) desde el equipo de usuario a la red. En la pasarela y en el equipo de usuario el tráfico de datos, que incluye una serie de paquetes de datos de IP (IP: "Internet Protocol", protocolo de internet) se puede filtrar utilizando filtros de paquetes de 5-tuplas de IP, dirigiendo de ese modo los paquetes de datos de IP a una portadora deseada.

Específicamente, se desea dirigir el tráfico de datos relativo a un servicio específico, por ejemplo TV móvil, a una portadora que ofrece una cierta QoS. Para este propósito, el tráfico de datos de DL puede estar sujeto a inspección de paquetes para identificar paquetes de datos relacionados con un servicio específico. Cuando se detectan paquetes de datos de un servicio predefinido, esto se puede señalizar a un controlador de políticas. El controlador de políticas puede generar a continuación filtros de paquetes correspondientes y señalizar estos filtros de paquetes a la pasarela. La pasarela utiliza a continuación los filtros de paquetes recibidos para encaminar los paquetes de datos a una portadora deseada. La portadora tiene habitualmente una clase de QoS que ha sido escogida por el operador de red para el servicio específico. En este proceso, puede haber asimismo señalización al equipo de usuario, por ejemplo para establecer una portadora e indicar filtros de paquetes de UL al equipo de usuario, que se deberían utilizar para encaminar tráfico de datos de UL sobre la portadora.

Sin embargo, la solución conocida puede tener problemas porque un servicio puede abrir o cerrar frecuentemente flujos de paquetes de IP asociados con el mismo servicio, por ejemplo tal como realizan ciertas aplicaciones de compartición de archivos entre pares. En este caso, el resultado sería una señalización considerable para establecer los filtros de paquetes con el fin de encaminar los paquetes de datos sobre la portadora deseada. Además, el encaminamiento de tráfico de datos de DL utilizando filtros de paquetes basados en 5-tuplas de IP requiere considerables recursos de procesamiento en la pasarela. Asimismo, en algunos casos puede ser difícil o imposible para una función de inspección de paquetes describir suficientemente flujos de paquetes de IP asociados con un servicio específico y señalizar esto al controlador de políticas. Por ejemplo, éste puede ser el caso si los flujos de paquetes de IP están cifrados o si el servicio está asociado con una gran cantidad de flujos de paquetes de IP, por ejemplo en el caso de ciertas aplicaciones de compartición de archivos entre pares.

Por consiguiente, existe una necesidad de técnicas potentes y eficientes para gestionar tráfico de red, que permitan asignar tráfico de datos de un servicio específico a un nivel deseado de QoS.

En el documento 3GPP TS23.203 V7.5.0 (2007-12), se describe un diseño de políticas y control de cobros según el cual una función de políticas y ejecución de cobros (PCEF, policy and charging enforcement function) puede aplicar filtros de flujo de datos de servicio para identificar un flujo de datos de servicio. Dicho filtro de flujos de datos de servicio puede asimismo extender la inspección de paquetes más allá de la 5-tupla de IP. Los filtros de flujos de datos de servicio se utilizan para dirigir paquetes de datos de tráfico de enlace descendente a una portadora correspondiente para un equipo de usuario.

La utilización de filtros de paquetes para dirigir paquetes de datos a portadoras se describe asimismo en las memorias WO 2007/087828 A1 y US 2007/0081499 A1.

Compendio

De acuerdo con una realización de la invención, se da a conocer un procedimiento de gestión de tráfico de red según la reivindicación 1 y un componente de red según la reivindicación 10. Las reivindicaciones dependientes definen realizaciones adicionales de la invención.

El identificador puede ser un campo de Punto de código de servicios diferenciados en una sección de cabecera de los paquetes de datos.

El identificador puede estar asociado con una portadora que tiene una clase específica de calidad de servicio, y el filtro de paquetes puede estar configurado para encaminar paquetes de datos con el identificador a la portadora asociada.

El procedimiento puede comprender además marcar con dicho identificador los paquetes de datos de dicho tráfico de datos relacionado con el servicio.

El procedimiento puede comprender además generar datos de control de inspección de paquetes, en base a dichos datos de políticas, mapeando dichos datos de control de inspección de paquetes dicho dispositivo a dicho identificador.

El procedimiento puede comprender a además marcar los paquetes de datos de dicho tráfico de datos relacionado con el servicio, en base a los datos de control de la inspección de paquetes.

Según otra realización de la invención, se da a conocer un componente de red. El componente de red incluye una interfaz de datos de inspección de paquetes configurada para recibir datos de inspección de paquetes que indican tráfico de datos relacionado con el servicio, de por lo menos uno de un usuario específico y un servicio específico, y un controlador de políticas configurado para recibir datos de políticas relativos a dicho por lo menos uno del usuario y el servicio. Además, el componente de red incluye un generador de filtros configurado para determinar un filtro de paquetes en base a los datos de inspección de paquetes y a los datos de políticas, configurándose el filtro de paquetes para filtrar tráfico de datos en base a un identificador incluido en paquetes de datos del tráfico de datos relacionado con el servicio, en respuesta a la inspección de paquetes.

Breve descripción de los dibujos

La figura 1 muestra esquemáticamente un entorno de comunicación móvil en el que se pueden aplicar conceptos según las realizaciones de la invención a la gestión de tráfico de datos de DL.

La figura 2 muestra esquemáticamente un ejemplo de un paquete de datos tal como se utiliza en una realización de la invención.

La figura 3 muestra esquemáticamente otro ejemplo de un paquete de datos tal como se utiliza en una realización de la invención.

La figura 4 muestra esquemáticamente un campo de información en una sección de cabecera de paquetes de datos.

La figura 5 muestra un diagrama de flujo para ilustrar un procedimiento de gestión de tráfico de datos de DL, de acuerdo con una realización de la invención.

La figura 6 muestra esquemáticamente un entorno de comunicación móvil en el que se pueden aplicar conceptos según las realizaciones de la presente invención a la gestión de tráfico de datos de UL.

La figura 7 muestra esquemáticamente un identificador y un identificador complementario en paquetes de datos.

La figura 8 muestra un diagrama de flujo para ilustrar un procedimiento de gestión de tráfico de datos de UL.

Descripción detallada de realizaciones

En lo que sigue, se explicará la invención en mayor detalle haciendo referencia a realizaciones a modo de ejemplo y a los dibujos adjuntos. Las realizaciones mostradas se refieren a gestionar tráfico de datos en una red de comunicación móvil, por ejemplo de acuerdo con las especificaciones de 3GPP (Third Generation Partnership Project, proyecto de asociación de tercera generación). Sin embargo, se debe entender que los conceptos que se describen en la presente memoria pueden ser aplicados asimismo a otros tipos de redes de comunicaciones. En relación con las figuras 1 a 5, se describirán conceptos para gestionar tráfico de datos de DL, es decir hacia un equipo de usuario. En relación con las figuras 6 a 8, se describirán conceptos para gestionar tráfico de datos de UL, es decir desde un equipo de usuario. Por lo tanto, los conceptos de gestión de tráfico de datos de DL y los conceptos de gestión de tráfico de datos de UL se describirán por separado. No obstante, se debe entender que estos conceptos pueden ser aplicados independientemente o en combinación.

La figura 1 muestra esquemáticamente un entorno de comunicación móvil en el que el tráfico de datos de DL se gestiona de acuerdo con una realización de la invención.

El entorno de red incluye un equipo de usuario 10, que se puede denominar asimismo un terminal, y una serie de componentes de red 22, 24, 26, 30, 100. Entre estos componentes de red, hay una red de acceso radio (RAN, Radio Access Network) 22. La RAN está basada en cierto tipo o tipos de tecnología de acceso radio, por ejemplo GSM (Global System for Mobile communications, sistema global para comunicaciones móviles), EDGE (Enhanced Data Rate for GSM Evolution, velocidad de datos mejorada para evolución de GSM) o UMTS (Universal Mobile Telecommunications System, sistema universal de telecomunicaciones móviles). Aunque la RAN 22 se muestra como un único nodo, se debe entender que la RAN 22 puede estar formada de hecho por una serie de componentes, que no se explican más en la presente memoria. La RAN 22 está acoplada a un nodo de transporte 24, que a su vez está acoplado a una pasarela 26. En este caso, se debe entender que alternativamente puede estar acoplado más de un nodo de transporte 24 entre la RAN 22 y la pasarela 26, o que la RAN 22 puede estar acoplada directamente a la pasarela 26. La pasarela 26 puede ser un nodo de soporte GPRS pasarela (GGSN,

Gateway GPRS Support Node) que proporciona una conexión de servicios basados en GPRS (GPRS: "General Packet Radio Service", servicio general de paquetes por radio) a uno o varias redes de datos de paquetes externas. La pasarela 26 puede ser asimismo una pasarela de evolución de la arquitectura de sistema (SAE GW, System Architecture Evolution Gateway) según las especificaciones 3GPP.

Además, la red de comunicación móvil incluye un controlador de políticas 30, que está implementado como una función de políticas y reglas de cobro (PCRF, Policy and Charging Rules Function) según las especificaciones 3GPP, y un inspector de paquetes 100. El controlador de políticas puede estar implementado mediante hardware dedicado o como una función de software ejecutada por un procesador. El inspector de paquetes 100 puede estar implementado mediante hardware dedicado o como una función de software ejecutada por un procesador. El inspector de paquetes 100 puede estar configurado para implementar una inspección de paquetes profunda (DPI, Deep Packet inspection), que puede estar basada en examinar tanto una sección de cabecera como una sección de datos de un paquete de datos. Además, la inspección puede estar basada asimismo en la obtención de medidas heurísticas tales como el tiempo entre llegadas de paquetes, los patrones de envío y el tamaño de los paquetes. Dicha heurística se puede aplicar incluso en caso de cifrado. Las secciones de cabecera y las secciones de datos se pueden examinar en diferentes capas de protocolo, por ejemplo en la capa de aplicación o en capas inferiores, para identificar diferentes servicios y protocolos. La inspección se puede llevar a cabo asimismo con respecto a señalización de control relativa a sesiones. Sin embargo, se pueden implementar asimismo otros tipos de procesos de inspección de paquetes, por ejemplo basados simplemente en una inspección de una sección de cabecera.

La pasarela 26, el controlador de políticas 30 y el inspector de paquetes 100 se consideran habitualmente componentes de una red central.

El controlador de políticas 30 comunica con el inspector de paquetes 100 por medio del trayecto de señalización 5. El trayecto de señalización 5 se puede implementar utilizando la interfaz de Rx o la interfaz de Gx, según las especificaciones 3GPP. Además, el controlador de políticas 30 comunica con la pasarela 26 por medio de un trayecto de señalización 6, que se puede implementar utilizando la interfaz Gx según las especificaciones 3GPP.

El controlador de políticas 30 está acoplado además a una base de datos de suscripciones 32 y a una base de datos de políticas de servicio 34 por medio de un trayecto de señalización 8, por ejemplo implementado utilizando una interfaz Sp según las especificaciones 3GPP. Por lo tanto, el controlador de políticas 30 puede recibir datos de políticas relativos a un usuario específico y/o relativos a un servicio específico disponible en la red de comunicación móvil, por ejemplo TV móvil.

El controlador de políticas 30 proporciona por lo tanto interfaces para soportar los trayectos de señalización 5, 6, 8.

Tal como se muestra además, el tráfico de datos relacionado con el servicio, entre la red y el equipo de usuario 10 se lleva a cabo mediante una serie de portadoras 52, 54. El tráfico de datos relacionado con el servicio pertenece habitualmente a una o varias aplicaciones cliente/par 12 ejecutándose en el equipo de usuario 10. Las portadoras 52, 54 se establecen entre el equipo de usuario 10 y la pasarela 26. Las portadoras 52, 54 transportan tráfico de datos tanto en el sentido de DL como en el sentido de UL, es decir se puede considerar asimismo que se están formadas por una portadora de DL y una portadora de UL. Para soportar comunicación bidireccional sobre las portadoras 52, 54, el equipo de usuario 10 está dotado de una estructura de transceptor, es decir tanto de un receptor 14 para recibir paquetes de datos entrantes desde las portadoras 52, 54 como de un transmisor 16 para enviar paquetes de datos salientes sobre las portadoras 52, 54. Las portadoras 52, 54 pueden incluir una portadora por defecto, establecida en general para ofrecer servicios basados en paquetes al equipo de usuario 10, y una o varias portadoras dedicadas 54 que pueden tener un nivel de QoS diferente, por ejemplo un nivel de QoS mayor, que la portadora por defecto. Cada portadora 52, 54 puede estar asociada con un correspondiente perfil de QoS. Los parámetros del perfil de QoS pueden ser un identificador de clase de QoS (QCI, QoS class), una prioridad de asignación/retención (ARP, allocation/retention priority), una tasa de bits máxima (MBR, maximum bit rate) y/o una tasa de bits garantizada (GBR, guaranteed bit rate). Por consiguiente, cada portadora 52, 54 puede estar asociada con una correspondiente clase de QoS.

En el equipo de usuario 10, los paquetes de datos son encaminados a una portadora deseada 52, 54 utilizando filtros de paquetes de UL 62, 64 configurados correspondientemente. En la pasarela 26, los paquetes de datos son encaminados a las portadoras deseadas 52, 54 utilizando filtros de paquetes de DL 72, 74 configurados correspondientemente. Se pueden señalizar parámetros del perfil de QoS desde el controlador de políticas 30 a la pasarela 26 utilizando el trayecto de señalización 6. Análogamente, los filtros de paquetes de DL 72, 74 para su utilización en la pasarela 26 se pueden señalizar desde el controlador de políticas 30 a la pasarela 26 por medio del trayecto de señalización 6. En relación con los filtros de paquetes de UL 62, 64 utilizados en el equipo de usuario 10, éstos se pueden señalizar desde el controlador de políticas 30 por medio de la pasarela 26. Sin embargo, en otras realizaciones, tal como se explicará en mayor detalle en relación con las figuras 6 a 8, los filtros de paquetes de UL 62, 64 se pueden generar asimismo en respuesta a la recepción de tráfico de datos en el equipo de usuario 10.

En la red de comunicación móvil que se muestra en la figura 1, el tráfico de datos de DL del equipo de usuario 10 pasa por el inspector de paquetes 100 antes de ser recibido por la pasarela 26. El inspector de paquetes 100 identifica paquetes de datos pertenecientes a uno o varios servicios predefinidos y/o pertenecientes a un usuario

específico. Esto se puede conseguir en base a los datos de control de inspección de paquetes recibidos desde el controlador de políticas 30. Si se identifican paquetes de datos pertenecientes a un servicio predefinido específico, el inspector de paquetes 100 proporciona una indicación respectiva al controlador de políticas 30 enviando datos de inspección de paquetes. Además, el inspector de paquetes 100 incluye una función de marcado 120, que incluye un identificador en el paquete de datos inspeccionado. La función de marcado 120 puede ser implementada por un hardware dedicado o como una función de software que se ejecuta en un procesador. El identificador se selecciona de acuerdo con el servicio identificado al que pertenece el paquete de datos. Por ejemplo, los paquetes de datos que pertenecen a un cierto servicio de compartición de archivos pueden recibir un primer identificador, y los paquetes de datos que pertenecen a un cierto servicio de transferencia continua de multimedia pueden recibir un segundo identificador. Incluir el identificador en los paquetes de datos, o marcar los paquetes de datos, se consigue por lo tanto en base al resultado de la inspección de paquetes o puede incluso formar parte del proceso de inspección de paquetes. El identificador se puede incluir en los paquetes de datos configurando un campo de información en una sección de cabecera del paquete de datos, por ejemplo configurando un punto de código de servicios diferenciados (DSCP, differentiated services code point) específico. El mapeo de un servicio específico a un correspondiente identificador puede ser controlado dinámicamente por el controlador de políticas 30 utilizando los datos de control de la inspección de paquetes. De este modo, el mapeo entre un servicio específico y un identificador correspondiente se puede controlar dinámicamente en base a datos de políticas. Por ejemplo, el mapeo podría variar en función de la hora del día o del día de la semana.

En base a los datos de inspección de paquetes recibidos del inspector de paquetes 100 y en base a los datos de políticas, el controlador de políticas 30 controla la selección y/o la configuración de los filtros de paquetes de DL 72, 74 utilizados en la pasarela 26 para encaminar paquetes de datos a portadoras deseadas 52, 54. Para este propósito, el controlador de políticas 30 incluye un generador 35 de filtros. El generador de filtros puede estar implementado mediante hardware dedicado o como una función de software ejecutada por un procesador. El generador de filtros 35 puede construir los filtros de paquetes de DL, seleccionar filtros de paquetes de DL preconfigurados a partir de una lista y/o configurar filtros de paquetes de DL seleccionados. Los filtros de paquetes de DL 72, 74 filtran el tráfico de datos de DL en base al identificador que ha sido incluido en los paquetes de datos por el inspector de paquetes 100. Esto permite un proceso de filtrado muy eficiente y fiable, dado que los filtros de paquetes de DL 72, 74 tienen únicamente que tener en cuenta el identificador incluido por el inspector de paquetes 100. Por ejemplo, si el identificador es un DSCP en la sección de cabecera de los paquetes de datos, los filtros de paquetes de DL 72, 74 necesitan tan sólo analizar el campo de información de DSCP en la sección de cabecera de los paquetes de datos. De este modo, el tráfico de datos que pertenece a un servicio específico puede ser encaminado dinámicamente a una portadora deseada 52, 54 con una clase de QoS correspondiente.

En lo que sigue, se explicarán en mayor detalle conceptos de marcado de paquetes de datos inspeccionados, haciendo referencia a tipos de paquetes de datos a modo de ejemplo.

La figura 2 muestra esquemáticamente paquetes de datos de IP del tipo IP versión 4. Tal como se muestra, una sección de cabecera de los paquetes de datos incluye varios campos de información, que se denominan "Versión", "IHL (IP Header Length, longitud de cabecera de IP)", "Servicios diferenciados", "Longitud total", "Identificación", "Indicadores", "Desplazamiento de fragmento", "Tiempo de vida", "Protocolo", "Suma de comprobación de cabecera", "Dirección de origen", "Dirección de destino", "Opciones" y "Relleno". Se definen detalles relativos a estos campos 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 asimismo campos de información que se denominan "Puerto de origen" y "Puerto de destino". Se definen campos de información correspondientes, por ejemplo, mediante el protocolo de control de transporte (TCP, Transport Control Protocol) definido en la especificación RFC 793 y el protocolo de datagramas de usuario (UDP, User Datagram Protocol) que se define en la especificación RFC 768.

A continuación de la sección de cabecera, están dispuestos habitualmente paquetes de datos de IP en una sección de datos, en la que pueden estar incluidos diferentes tipos de tráfico de datos de carga útil.

La figura 3 muestra esquemáticamente paquetes de datos de IP de acuerdo con el tipo de IP versión 6. De nuevo, la sección de cabecera incluye una serie de campos de información, que se denominan "Versión", "Servicios diferenciados", "Etiqueta de flujo", "Longitud de carga útil", "Siguiente cabecera", "Límite de saltos", "Dirección de origen" 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 asimismo campos de información denominados "Puerto de origen" y "Puerto de destino", por ejemplo tal como se define mediante TCP o UDP. De nuevo, la sección de cabecera estará seguida habitualmente por una sección de datos que puede llevar varios tipos de datos de carga útil.

Para los objetivos de la presente descripción, se explicarán en mayor detalle solamente los campos de información denominados "Servicios diferenciados", "Dirección de origen", "Dirección de destino", "Puerto de origen" y "Puerto de destino". En relación con los otros campos de información, se pueden extraer explicaciones adicionales de las especificaciones RFC mencionadas anteriormente.

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

El campo de información "Puerto de origen" indica un número de puerto en el origen 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.

En base a la dirección de origen, a la dirección de destino, al puerto de origen y al puerto de destino, un flujo de paquetes IP se puede definir como un flujo de paquetes IP entre un primer punto extremo definido por la dirección de origen y el puerto de origen, y un segundo punto extremo definido por la dirección de destino y el puerto de destino. Una entidad que incluye la dirección de origen, la dirección de destino, el puerto de origen, el puerto de destino y un identificador de protocolo se denomina asimismo una "5-tupla de IP".

El campo de información "Servicios diferenciados" está incluido tanto en los paquetes de datos de IP versión 4 como en los paquetes de datos de IP versión 6. Tal 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 muestra esquemáticamente en la figura 4.

Tal como se muestra en la figura 4, se utilizan seis bits del campo de información, es decir los bits 0 a 5, para definir el Punto de código de servicios diferenciados (DSCP). Los otros dos bits nos utilizan. Utilizando el DSCP, se puede controlar el envío de paquetes de datos mediante nodos de red. Para paquetes de datos que pertenecen a diferentes tipos de servicios se pueden seleccionar procedimientos de transmisión diferentes. Los DSCP pueden estar estandarizados. Además, está disponible una amplia gama de DSCP no estandarizados.

En lo que sigue, se describirá en mayor detalle un proceso de gestión de tráfico de datos de DL, de acuerdo con una realización de la invención. Esto se llevará a cabo haciendo referencia al entorno de red de comunicación móvil que se muestra en la figura 1.

Tal como se ha mencionado anteriormente, la red de comunicación móvil puede soportar una serie de clases de QoS asociadas con diferentes portadoras. Las clases de QoS se pueden identificar mediante un QCI correspondiente. Para marcar paquetes de datos identificados de un servicio específico en el inspector de paquetes 100, se define un DSCP dedicado, por ejemplo a partir de la gama de DSCP no estandarizados. Como resultado, puede haber un DSCP dedicado por cada portadora.

Además, se define una tabla de mapeo que mapea cada servicio a detectar por el inspector de paquetes 100 a un DSCP dedicado. Por lo tanto, pueden ser utilizados diferentes DSCP dedicados para marcar paquetes de datos pertenecientes a diferentes servicios. Sin embargo, es posible asimismo que se marquen paquetes de datos de diferentes servicios con el mismo DSCP, por ejemplo si estos servicios deberían ser asignados a la misma clase de QoS. Esta tabla de mapeo puede estar mantenida por el controlador de políticas 30 y además ser comunicada al inspector de paquetes 100, por ejemplo utilizando el trayecto de señalización 5. Alternativamente, el inspector de paquetes 100 puede asimismo configurarse de manera estática con la tabla de mapeo. Si la tabla de mapeo en el inspector de paquetes 100 es configurable dinámicamente mediante el controlador de políticas 30, es posible asimismo reconfigurar la tabla de mapeo en base a datos de políticas. Por ejemplo, la tabla de mapeo se podría reconfigurar en función de la hora del día o en función del día de la semana.

Si el inspector de paquetes 100 detecta un flujo de paquetes IP perteneciente a un servicio predefinido, esto se señaliza al controlador de políticas 30 en los datos de inspección de paquetes. Además, la función de marcado 120 del inspector de paquetes 100 marca los paquetes de datos pertenecientes al servicio con el DSCP que se ha definido en la tabla de mapeo. Para otros paquetes de datos, es decir paquetes de datos que no están identificados como pertenecientes a un servicio predefinido, se puede configurar un DSCP por defecto. Por ejemplo, el DSCP por defecto puede ser cero. Como alternativa, se puede omitir la configuración de un DSCP para paquetes de datos que no estén identificados como pertenecientes a un servicio predefinido. En los datos de inspección de paquetes, el inspector de paquetes 100 puede asimismo señalizar un identificador de servicio al controlador de políticas 30. Por medio del identificador de servicio, el servicio identificado y/o el DSCP utilizado para marcar los correspondientes paquetes de datos se pueden señalizar al controlador de políticas 30. La activación, basada en frecuencias o en eventos, de señalización hacia el controlador de políticas 30 se puede seleccionar adecuadamente.

En respuesta a los datos de inspección de paquetes, el controlador de políticas 30 determina un filtro de paquetes de DL que funciona en base al DSCP utilizado para el marcado de paquetes de datos del servicio identificado. De acuerdo con una realización, el filtro de paquetes de DL puede funcionar sustancialmente sólo en base al DSCP utilizado para marcar los paquetes de datos. El filtro de paquetes de DL se señaliza a la pasarela 26.

Utilizando el filtro de paquetes de DL, la pasarela 26 encamina a continuación los paquetes de datos de DL que están marcados con el DSCP, a la portadora correspondiente 52, 54. Ésta puede ser una portadora 52, 54 ya existente. Si la portadora no existe, ésta se puede establecer a la recepción de la señalización desde el controlador de políticas 30. Es decir, si está establecida ya una portadora 52, 54 que tiene la clase de QoS asociada con el

DSCP, el filtro de paquetes de DL encaminará los paquetes de datos filtrados a esta portadora ya existente. Si no existe dicha portadora, se establecerá una portadora de la clase de QoS asociada con el DSCP, a la recepción de la señalización de filtro de paquetes de DL desde el controlador de políticas 30.

La figura 5 muestra un diagrama de flujo para ilustrar esquemáticamente un procedimiento 200 de gestión de tráfico de datos de DL, de acuerdo con los conceptos mencionados anteriormente.

En la etapa 210, se reciben datos de inspección de paquetes, por ejemplo en el controlador de políticas 30. Los datos de inspección de paquetes recibidos pueden incluir un identificador de servicio que indica un servicio al que pertenecen los paquetes de datos identificados. Además, los datos de inspección de paquetes pueden indicar un identificador que se utiliza para marcar los paquetes de datos en respuesta a la inspección de paquetes, por ejemplo un DSCP dedicado.

En la etapa 220, se reciben datos de políticas. Los datos de políticas pueden incluir políticas generales definidas por un operador de una red de comunicación móvil sobre cómo gestionar paquetes de datos de un servicio específico, o pueden estar relacionados con el usuario, es decir, definir cómo gestionar paquetes de datos de un servicio específico y un usuario específico. Los datos de políticas pueden distinguir asimismo entre diferentes grupos de abonados o pueden definir una cuota de volumen de un usuario, abonado, grupo de abonados o servicio. Específicamente, los datos de políticas pueden indicar qué clase de calidad de servicio se debería proporcionar a paquetes de datos pertenecientes a un servicio específico. Esta información puede variar dinámicamente, por ejemplo en base a la hora del día, al día de la semana, o a la cuota de volumen utilizada.

En la etapa 230, se determina el filtro de paquetes de DL en base a los datos de inspección de paquetes y a los datos de políticas. En particular, se determina un filtro de paquetes de DL que funciona en base a un identificador incluido en los paquetes de datos en respuesta al proceso de inspección de paquetes. El filtro de paquetes de DL se utiliza a continuación para encaminar los paquetes de datos marcados a una portadora que tiene la clase de QoS deseada. Para este propósito, el filtro de paquetes de DL determinado se puede señalizar desde un controlador de políticas, por ejemplo el controlador de políticas 30, a una pasarela, por ejemplo la pasarela 26.

La figura 6 muestra esquemáticamente un entorno de comunicación móvil en el que el tráfico de datos de UL se gestiona de acuerdo con una realización de la invención. El entorno de comunicación móvil de la figura 6 es similar en general al de la figura 1, y los componentes similares se han indicado con signos de referencia similares. Para más detalles, se hace referencia a las explicaciones correspondientes en relación con la figura 1.

De acuerdo con los conceptos que se muestran en la figura 6, la información de los paquetes de datos de DL se utiliza en el equipo de usuario 10 para formar reglas locales para encaminar paquetes de datos de UL. En este caso, se debe observar que en un escenario de comunicación móvil, el flujo de paquetes de datos de IP es habitualmente bidireccional. Incluso si el transporte de datos de carga útil se produce solamente en un sentido, por ejemplo en base a paquetes TCP, el flujo de paquetes de IP incluirá asimismo habitualmente paquetes de control, por ejemplo paquetes de acuse de recibo TCP, transmitidos en el sentido opuesto. Además, las direcciones IP de origen y de destino, y los números de puerto de un flujo de paquetes IP son habitualmente simétricos, es decir el punto extremo de destino (identificado por una dirección IP y un número de puerto) en un sentido es el mismo que el punto extremo de origen (identificado por dirección IP y número de puerto) en el sentido opuesto, y viceversa. Debido a la simetría, los paquetes del mismo flujo de paquetes de IP que fluyen en sentidos opuestos tendrán identificadores de dirección "complementarios", e identificadores de puerto "complementarios", lo que significa que el identificador de origen en un sentido es el mismo que el identificador de destino en el sentido contrario.

De acuerdo con los conceptos de gestión de tráfico de datos de UL que se explican a continuación, se supondrá que el tráfico de datos de DL está ya mapeado a clases de QoS y portadoras correspondientes. Esto se puede conseguir de acuerdo con los conceptos explicados anteriormente en relación con la figura 1. Es decir, el entorno de comunicación móvil de la figura 6 podría incluir asimismo el inspector de paquetes 100 y funcionalidades asociadas para gestionar tráfico de datos de DL según se ha explicado en relación con la figura 1. No obstante, se debe entender que son aplicables asimismo otros conceptos de mapeo de tráfico de datos de DL a clases de QoS y portadoras.

Tal como se muestra en la figura 6, el equipo de usuario 10 incluye además una función de réplica 220. La función de réplica 220 puede ser implementada por un hardware dedicado o como una función de software que se ejecuta en un procesador. La función de réplica 220 está configurada para detectar paquetes de datos entrantes que incluyen un primer identificador y paquetes de datos salientes que incluyen un segundo identificador que es complementario con respecto al primer identificador. En el identificador complementario, un identificador de punto extremo de destino, por ejemplo dirección IP de destino y/o puerto de destino, es el mismo que un identificador del punto extremo de origen, por ejemplo dirección IP de origen y/o puerto de origen, en el identificador. Cada uno del primer y el segundo identificadores pueden ser una 5-tupla de IP. La función de réplica 220 controla los filtros de paquetes de UL 62, 64, que están basados en 5-tuplas de IP, de tal modo que los paquetes de datos salientes que tienen el segundo identificador complementario son encaminados a la misma portadora desde la que se reciben los paquetes de datos entrantes que tienen el primer identificador. De este modo, no es necesaria ninguna señalización explícita entre la pasarela 26 y el equipo de usuario 10 para seleccionar o configurar los filtros de paquetes de UL

62, 64. Si la función réplica 220 detecta que se ha mapeado un nuevo flujo de paquetes de IP sobre una portadora 52, 54 o que se ha establecido una nueva portadora 52, 54, la función réplica 220 generará automáticamente un correspondiente filtro de paquetes de UL 62, 64. Si se identifican paquetes de datos en el sentido de DL mediante una 5-tupla de IP específica, el filtro de paquetes de UL 62, 64 estará configurado para encaminar paquetes de datos salientes que llevan una 5-tupla de IP complementaria, a la misma portadora desde la que se reciben los paquetes de datos entrantes.

La estructura de un identificador y un identificador complementario, que están basados en la 5-tupla de IP, se muestra en la figura 7. Sin embargo, se debe entender que son asimismo posibles otros tipos de identificadores e identificadores complementarios. En general, el identificador complementario indica el origen identificado en el identificador de un paquete de datos entrante como el destino de un paquete de datos saliente.

Tal como se muestra en la figura 7, un identificador en la base de la 5-tupla de IP puede incluir una dirección de origen A, una dirección de destino B, un puerto de origen C, un puerto de destino D y un identificador de protocolo X. El correspondiente identificador complementario tendrá entonces una dirección de origen B, una dirección de destino A, un puerto de origen D, un puerto de destino C y un identificador de protocolo X. En otras palabras, en el identificador complementario la dirección de origen y la dirección de destino están intercambiadas en comparación con el identificador. Análogamente, en el identificador complementario, el puerto de origen y el puerto de destino están intercambiados en comparación con el identificador. El identificador de protocolo permanece invariable. En otras realizaciones, pueden ser utilizados diferentes tipos de identificador e identificador complementario, por ejemplo en base a solamente una parte de la 5-tupla de IP. Por ejemplo, en el identificador complementario, se podrían intercambiar solamente la dirección de origen y la dirección de destino, en comparación con el identificador.

En lo que sigue, se explicará en mayor detalle un proceso de gestión de paquetes de datos de UL de acuerdo con una realización de la invención, haciendo referencia a las estructuras que se muestran en la figura 6.

Inicialmente, los paquetes de datos de UL relacionados con un servicio específico pueden ser transmitidos desde el equipo de usuario 10 a la pasarela 26 sobre una portadora arbitraria, por ejemplo sobre la portadora por defecto. Entonces, el correspondiente flujo de paquetes IP incluirá asimismo paquetes de datos transmitidos en el sentido de DL. Estos paquetes de datos serán mapeados a una clase de QoS deseada y la portadora correspondiente 52, 54, por ejemplo utilizando los conceptos que se han explicado en relación con la figura 1. Este proceso puede involucrar asimismo el establecimiento de una nueva portadora asociada con la clase de QoS deseada.

La función de réplica 220 en el equipo de usuario 10 detecta a continuación los paquetes de datos entrantes que se reciben de esta portadora 52, 54 y genera un filtro de paquetes de UL "replicado" 62, 64, que funciona en la base de una 5-tupla de IP que es complementaria a una 5-tupla de IP de los paquetes de datos entrantes recibidos. En este caso, se debe entender que pueden estar presentes diferentes flujos de paquetes IP en una única portadora 52, 54, y que múltiples filtros de paquetes de UL 62, 64 pueden encaminar paquetes de datos salientes sobre la misma portadora 52, 54. Si hay un nuevo flujo de paquetes IP con paquetes de datos entrantes sobre una portadora 52, 54 o se establece una nueva portadora, se generará un correspondiente filtro de paquetes de datos de UL nuevo 62, 64.

Cuando se aplican los conceptos mencionados anteriormente, el equipo de usuario 10 puede recibir una funcionalidad para indicar a la red de comunicación móvil que soporta la función de réplica 220. Por ejemplo, esto se podría incluir en señalización de gestión de sesiones, por ejemplo durante un procedimiento de acoplamiento entre el equipo de usuario 10 y la red central. A modo de ejemplo, se podría añadir un elemento de información al proceso de señalización, en el que el equipo de usuario 10 puede indicar que soporta a la función de réplica 220. La figura 6 muestra esquemáticamente un correspondiente trayecto de señal 2 que se extiende desde el equipo de usuario 10. En este caso, se debe entender que el trayecto de señalización 2 se representa esquemáticamente extendiéndose desde el equipo de usuario 10 directamente a un nodo de red específico, por ejemplo al controlador de políticas 30 mostrado, pero habitualmente puede estar implementado a través de otros nodos de red. Por ejemplo, en una red de comunicación UMTS, el trayecto de señalización 2 se podría extender desde el equipo de usuario 10 hasta un nodo de soporte GPRS de servicio (SGSN, Serving GPRS Support Node). En una red de comunicación de evolución a largo plazo/evolución de arquitectura de servicio (SAE/LTE, Long Term Evolution/Service Architecture Evolution), el trayecto de señalización 2 se podría extender desde el equipo de usuario 10 hasta una entidad de gestión móvil (MME, Mobile Management Entity). Desde estos nodos de red, la información de señalización puede a continuación ser transmitida o distribuida otros nodos de red, por ejemplo al controlador de políticas 30.

En algunas realizaciones, la información de que el equipo de usuario 10 soporta la función de réplica 220 puede ser distribuida asimismo entre nodos de la red central, por ejemplo al controlador de políticas 30 o a un nodo que soporta una función de inspección de paquetes, por ejemplo el inspector de paquetes 100 que se muestra en la figura 1. Para este propósito, se puede reutilizar la interfaz Gx o la interfaz Rx según las especificaciones 3GPP.

De acuerdo con algunas realizaciones, se puede disponer otro trayecto de señalización 4 desde la red de comunicación móvil hasta el equipo de usuario 10. Utilizando este trayecto de señalización 4, puede ser posible activar o desactivar la función de réplica 220 para cada portadora. Esto puede ser útil si no todas las aplicaciones o servicios requieren la activación de esta función. Por ejemplo, en algunos casos la 5-tupla de IP en los paquetes de

datos de un servicio se puede definir estadísticamente y se puede utilizar un correspondiente filtro de paquetes de UL estático 62, 64 en el equipo de usuario 10. De nuevo, se debe entender que el trayecto de señalización 4 se representa esquemáticamente extendiéndose hasta el equipo de usuario 10 directamente desde un nodo de red específico, por ejemplo desde el controlador de políticas 30 mostrado, pero habitualmente puede estar implementado a través de otros nodos de red. Por ejemplo, en una red de comunicación UMTS, el trayecto de señalización 2 se podría extender desde un nodo de soporte GPRS de servicio (SGSN, Serving GPRS Support Node) hasta el equipo de usuario 10. En una red de comunicación de evolución a largo plazo/evolución de arquitectura de servicio (SAE/LTE), el trayecto de señalización 2 se podría extender desde una entidad de gestión móvil (MME) hasta el equipo de usuario 10. A su vez, estos nodos de red pueden recibir la información de señalización desde otros nodos de la red, por ejemplo el controlador de políticas 30.

En algunas realizaciones, la red de comunicación móvil puede señalizar al equipo de usuario 10 si debería o no aplicarse la función de réplica 220, por ejemplo utilizando procedimientos estándar de establecimiento o modificación de portadoras, tal como se define en las especificaciones 3GPP. Se podría añadir un correspondiente elemento de información para este propósito, a los procedimientos estandarizados de establecimiento o modificación de portadoras. En estos casos, la señalización desde el equipo de usuario 10 a la red de comunicación móvil indicando que está soportada la función de réplica 220 se podría implementar asimismo en función de cada portadora. Es decir, la correspondiente señalización podría especificar el soporte de la función de réplica 220 para una nueva portadora o podría modificar la información de soporte para una portadora ya establecida.

La figura 8 muestra un diagrama de flujo que ilustra un procedimiento 300 para gestionar tráfico de datos de UL, de acuerdo con los conceptos mencionados en lo anterior.

En la etapa 310, se reciben desde una portadora paquetes de datos entrantes con un primer identificador. Tal como se ha explicado anteriormente, la portadora puede estar asociada con una clase de QoS correspondiente, y el primer identificador puede ser una 5-tupla de IP.

En la etapa 320, se detectan paquetes de datos salientes con un segundo identificador, complementario. Esto se puede conseguir generando o configurando un filtro de paquetes de UL "replicado" que funciona sobre la base de una 5-tupla de IP que es complementaria a la 5-tupla de IP de los paquetes de datos entrantes recibidos de la portadora.

En la etapa 330, se encaminan paquetes de datos salientes con el segundo identificador a la misma portadora desde la que se reciben los paquetes de datos entrantes con el primer identificador. De nuevo, esto se puede conseguir seleccionando o configurando un correspondiente filtro de paquetes de UL "replicado", por ejemplo actuando sobre la base del identificador complementario o una parte del mismo.

De acuerdo con los conceptos que se han explicado anteriormente, es posible mapear dinámicamente tráfico de datos relacionado con el servicio a una clase de QoS deseada, por ejemplo en base a datos de políticas específicos del usuario y/o en base a datos de políticas específicos del servicio. Además, este mapeo podría depender de la hora del día, del día de la semana o de otros parámetros. Se pueden definir por lo tanto diversas políticas diferentes en los datos de políticas para controlar el mapeo del tráfico de datos relacionado con el servicio a una clase de QoS. Una de dichas políticas puede ser incluso bloquear el tráfico de datos relativo a un servicio específico en la pasarela.

Además, el control de la QoS en base a los datos de políticas se puede conseguir de manera eficiente, sin requerir demasiada señalización sobre interfaces de la red central o al equipo de usuario. Cuando se combinan los conceptos de gestión de tráfico de datos de DL que se han explicado en relación con las figuras 1 a 5, con los conceptos de gestión de tráfico de datos de UL que se han explicado en relación con las figuras 6 a 8, se obtiene una solución eficiente que permite la gestión tanto de tráfico de datos de DL como de tráfico de datos de UL.

Además, los conceptos que se han descrito anteriormente no dependen del establecimiento de portadoras que no son necesarias. Por el contrario, las portadoras se pueden establecer cuando se necesitan, utilizando por lo tanto de manera eficiente los recursos de red disponibles.

Se debe entender que los conceptos que se han explicado anteriormente son tan sólo a modo de ejemplo y susceptibles de diversas modificaciones. Por ejemplo, los nodos de red que se muestran en las figuras 1 y 6 no tienen que implementarse como nodos independientes, sino que se pueden integrar en un único componente de red. Por ejemplo, el inspector de paquetes 100 podría asimismo estar integrado en la pasarela 26. Los conceptos se pueden aplicar en varios tipos de redes de comunicación móvil. Finalmente, se debe observar que la solución para la gestión de tráfico de datos de UL explicada en relación con las figuras 6 a 8 no se limita a la gestión de tráfico de datos de UL procedente de un equipo de usuario. Por el contrario, estos conceptos se pueden aplicar en general a todas las situaciones en las que ya están mapeados paquetes de datos entrantes a una portadora específica y existen correspondientes paquetes de datos salientes.

REIVINDICACIONES

1. Un procedimiento de gestión de tráfico de red, comprendiendo el procedimiento:

- un inspector de paquetes (100) que lleva a cabo la inspección de paquetes de un paquete de datos de tráfico de datos de enlace descendente hacia un equipo de usuario (10);

- identificando el inspector de paquetes (100) que el paquete de datos pertenece a un servicio predefinido específico;

- enviando el inspector de paquetes (100) datos de inspección de paquetes a un controlador de políticas (30), indicando los datos de inspección de paquetes tráfico de datos relacionado con el servicio, de un servicio predefinido específico, e incluyendo un identificador de servicio que indica el servicio al que pertenece el paquete de datos identificado; y

- marcando el inspector de paquetes (100) el paquete de datos identificado mediante incluir un identificador en el paquete de datos identificado.

2. El procedimiento según la reivindicación 1,

en el que la inspección de paquetes se lleva a cabo mediante la inspección de una sección de cabecera del paquete de datos.

3. El procedimiento según la reivindicación 1 ó 2,

en el que la inspección de paquetes se lleva a cabo mediante la inspección tanto de una sección de cabecera como de una sección de datos del paquete de datos.

4. El procedimiento según cualquiera de las reivindicaciones anteriores,

en el que dicho identificador se incluye configurando un campo de Punto de código de servicios diferenciados en una sección de cabecera de los paquetes de datos.

5. El procedimiento según cualquiera de las reivindicaciones anteriores,

en el que los datos de inspección de paquetes indican el identificador que se utiliza para el marcado de los paquetes de datos.

6. El procedimiento según cualquiera de las reivindicaciones anteriores, que comprende:

- la recepción, mediante el inspector de paquetes (100), de datos de control de inspección de paquetes desde el controlador de políticas (30), mapeando dichos datos de control de inspección de paquetes dicho servicio predefinido específico a dicho identificador.

7. El procedimiento según la reivindicación 6,

en el que el mapeo se define en una tabla de mapeo.

8. El procedimiento según la reivindicación 6 ó 7,

en el que el mapeo varía en función de la hora del día o del día de la semana.

9. El procedimiento según cualquiera de las reivindicaciones 6 a 8, que comprende:

- el marcado, por el inspector de paquetes (100), de los paquetes de datos de dicho tráfico de datos relacionado con el servicio, en base a los datos de control de la inspección de paquetes.

10. Un componente de red, que comprende:

- un inspector de paquetes (100) configurado para llevar a cabo la inspección de paquetes de un paquete de datos de tráfico de datos de enlace descendente hacia un equipo de usuario (10), con el fin de identificar que el paquete de datos pertenece a un servicio predefinido específico, y para marcar el paquete de datos identificado incluyendo un identificador en el paquete de datos identificado;

y

- una interfaz (5) de datos de inspección de paquetes configurada para enviar, a un controlador de políticas (30), datos de inspección de paquetes que indican tráfico de datos relacionado con el servicio, del servicio específico e incluyen un identificador de servicio que indica el servicio al que pertenece el paquete de datos identificado.

11. El componente de red según la reivindicación 10,

en el que el inspector de paquetes (100) está configurado para llevar a cabo todas las etapas del procedimiento según cualquiera de las reivindicaciones 1 a 9.

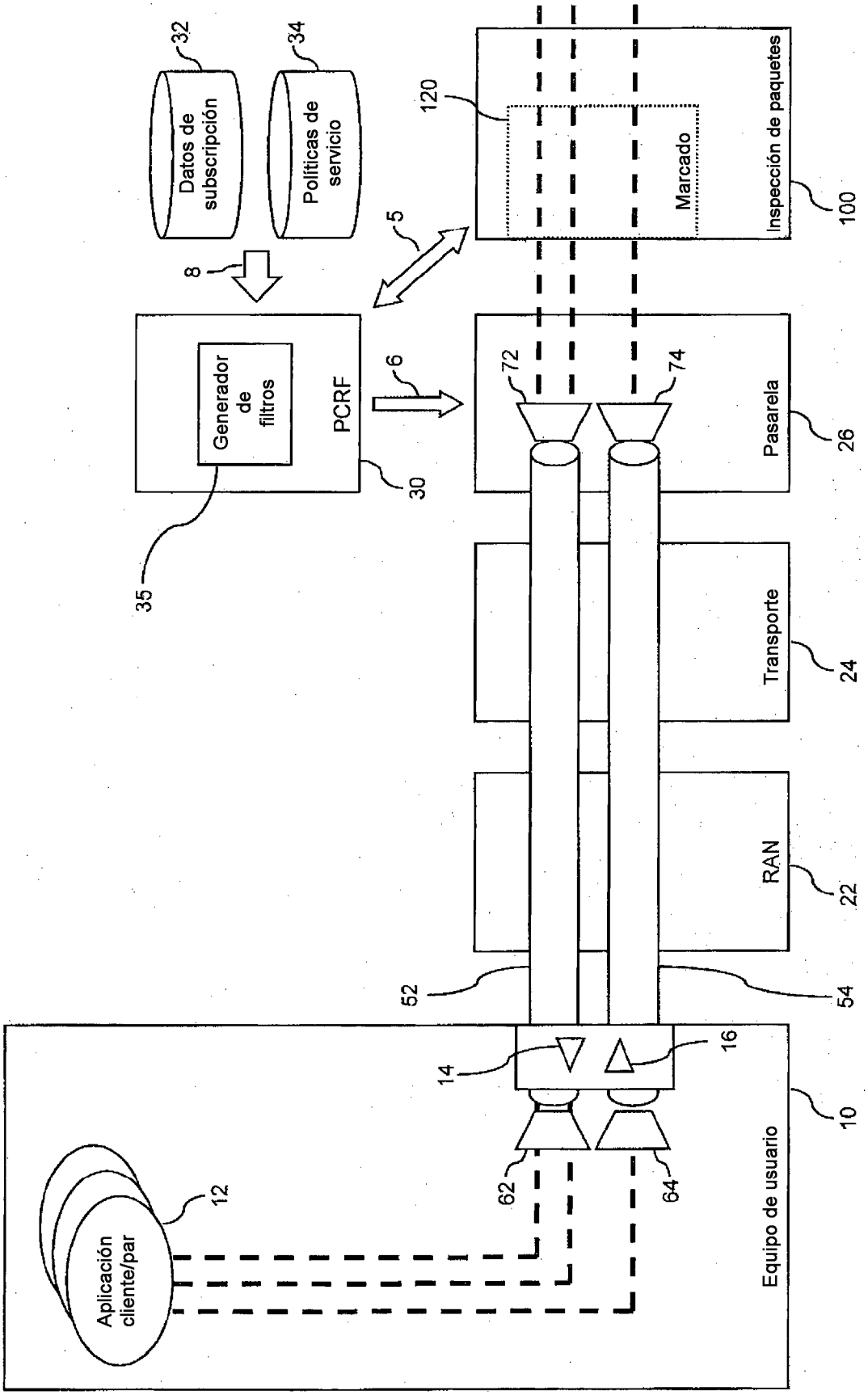
32
Datos de subscripción
34
Políticas de servicio
120
Marcado
Inspección de paquetes
100
5
8
Generador de filtros
PCRF
30
6
72
74
Pasarela
26
35
Transporte
24
RAN
22
52
54
14
16
62
64
Equipo de usuario
10
12
Aplicación cliente/par

FIG. 1

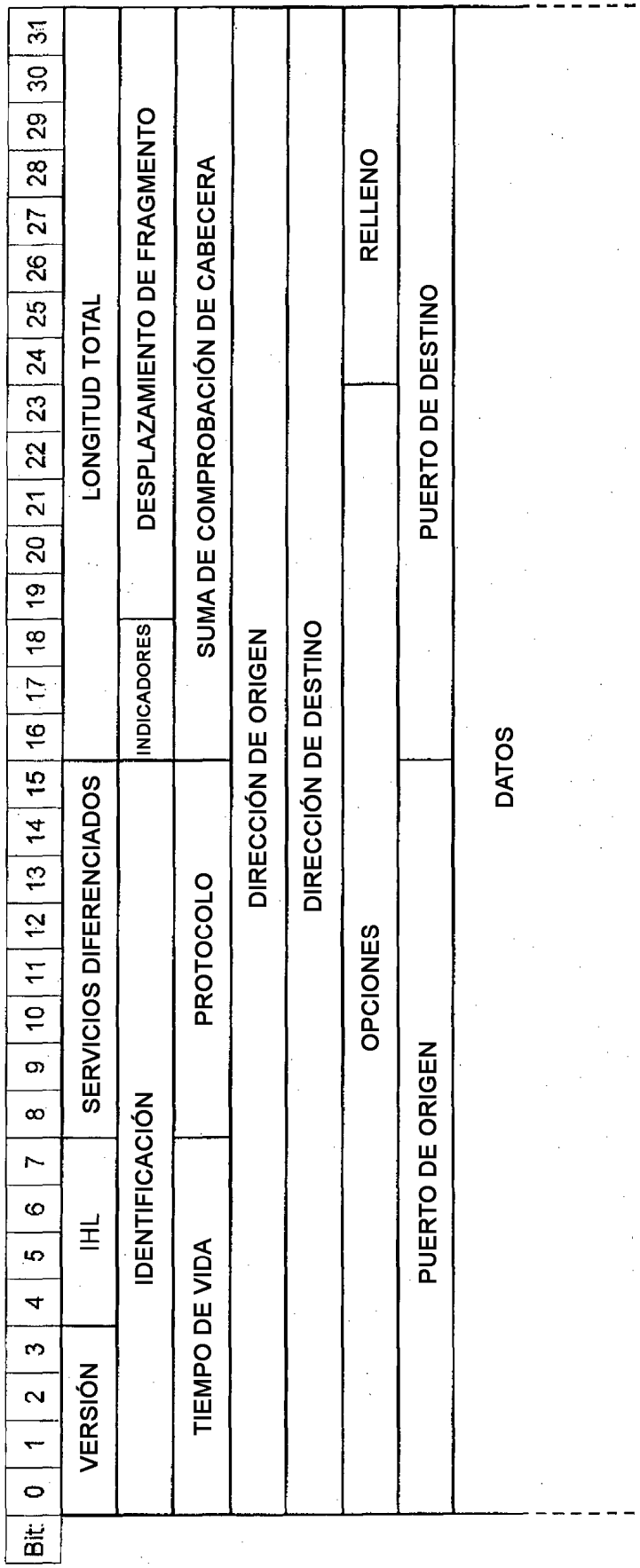
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSIÓN
IHL
SERVICIOS DIFERENCIADOS
LONGITUD TOTAL
IDENTIFICACIÓN
INDICADORES
DESPLAZAMIENTO DE FRAGMENTO
TIEMPO DE VIDA
PROTOCOLO
SUMA DE COMPROBACIÓN DE CABECERA
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
OPCIONES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

FIG. 2

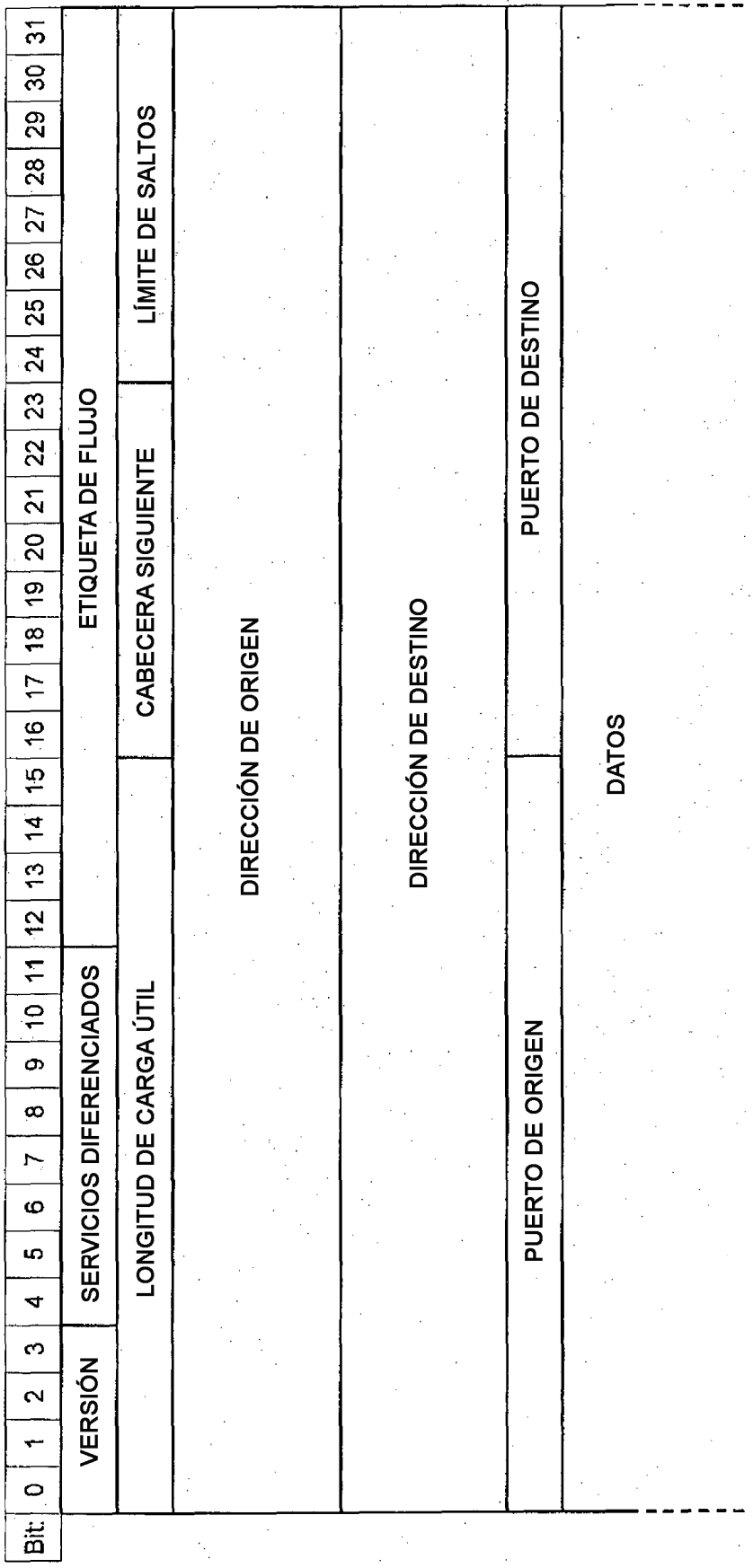
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSIÓN
SERVICIOS DIFERENCIADOS
ETIQUETA DE FLUJO
LONGITUD DE CARGA ÚTIL
CABECERA SIGUIENTE
LÍMITE DE SALTOS
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
PUERTO DE ORIGEN
PUERTO DE DESTINO
DATOS

FIG. 3

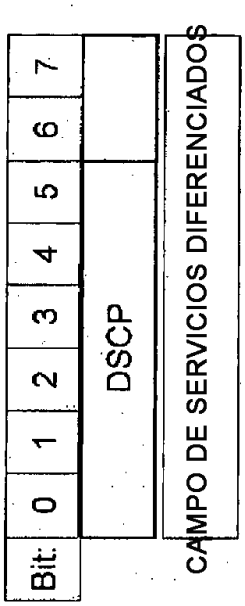

FIG. 4

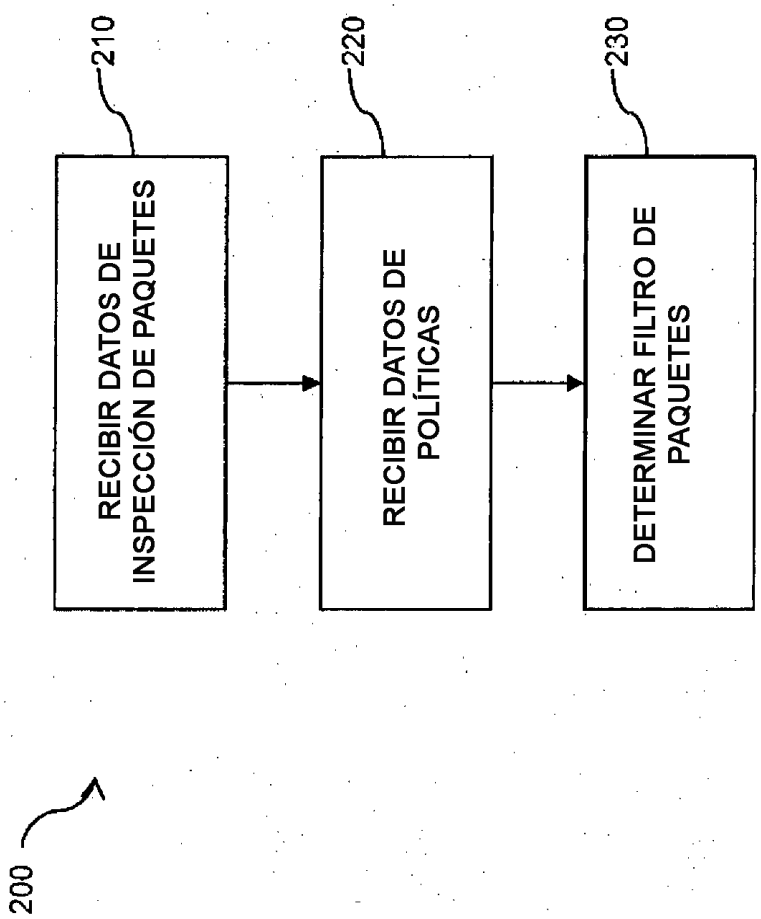
210
220
230
RECIBIR DATOS DE INSPECCIÓN DE PAQUETES
RECIBIR DATOS DE POLÍTICAS
DETERMINAR FILTRO DE PAQUETES
200

FIG. 5

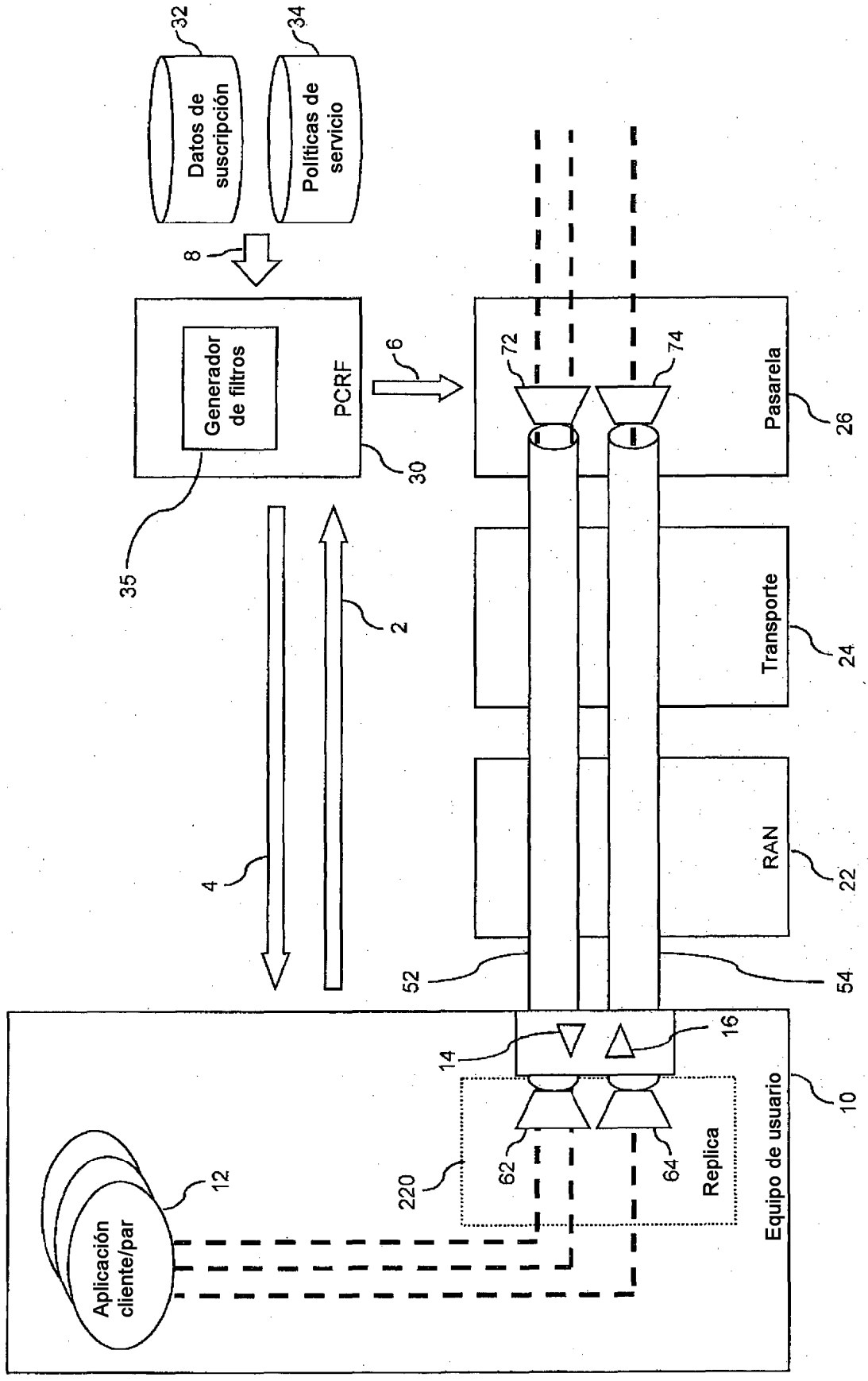
32
34
Datos de suscripción
Políticas de servicio
8
Generador de filtros
PCRF
6
30
35
2
4
72
74
Pasarela
26
Transporte
24
RAN
22
52
54
14
16
Equipo de usuario
10
220
62
64
Replica
12
Aplicación cliente/par

FIG. 6

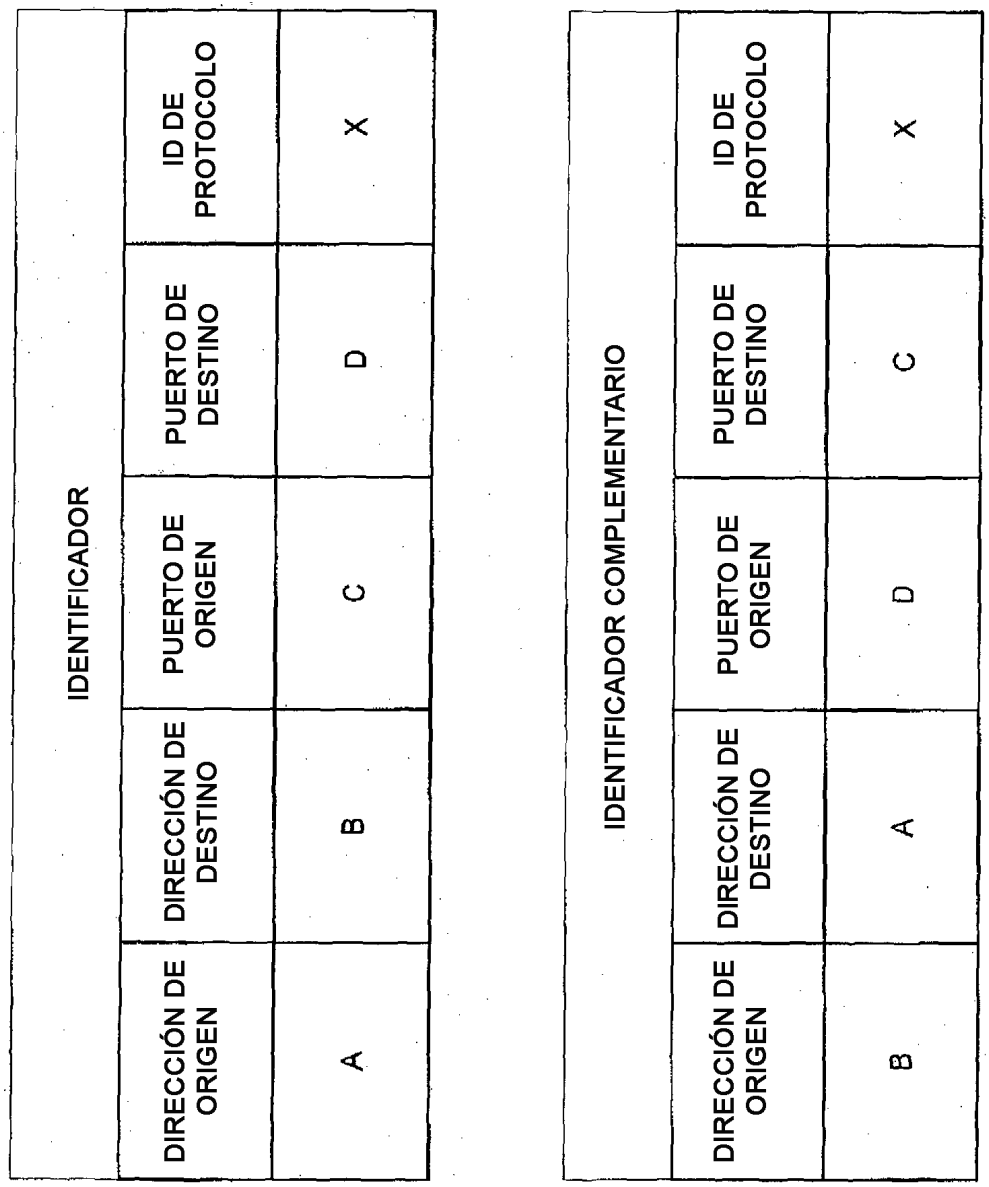
IDENTIFICADOR
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
PUERTO DE ORIGEN
PUERTO DE DESTINO
ID DE PROTOCOLO
A
B
C
D
X
IDENTIFICADOR COMPLEMENTARIO
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
PUERTO DE ORIGEN
PUERTO DE DESTINO
ID DE PROTOCOLO
B
A
D
C
X

FIG. 7

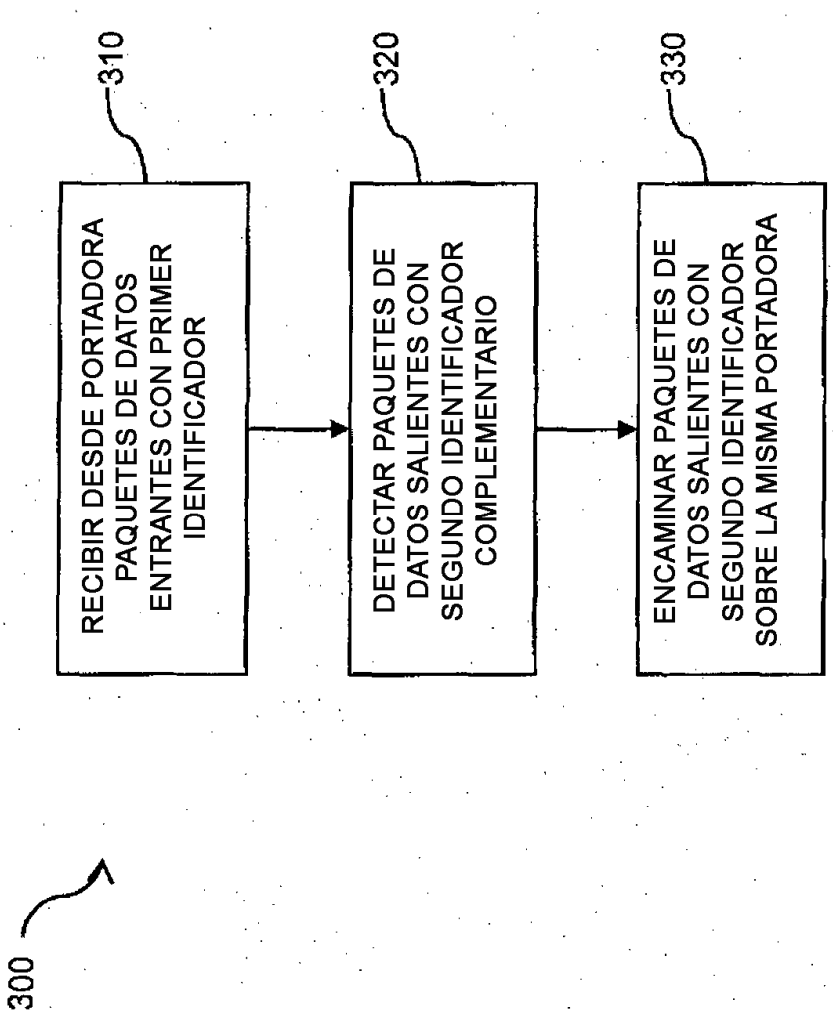
300
310
RECIBIR DESDE PORTADORA PAQUETES DE DATOS ENTRANTES CON PRIMER IDENTIFICADOR
320
DETECTAR PAQUETES DE DATOS SALIENTES CON SEGUNDO IDENTIFICADOR COMPLEMENTARIO
330
ENCAMINAR PAQUETES DE DATOS SALIENTES CON SEGUNDO IDENTIFICADOR SOBRE LA MISMA PORTADORA

FIG. 8