(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 758 190**

(51) Int. CI.:

H04W 28/18 (2009.01)
H04W 72/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.04.2009 E 17174284 (4)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2019 EP 3236690**

(54) Título: **Técnicas de gestión del tráfico de red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2020

(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

Técnicas de gestión del tráfico de red

Campo técnico

La presente invención versa sobre técnicas para gestionar el tráfico de red.

Antecedentes

En las redes de comunicaciones móviles se sabe dirigir tráfico de red relativo a un servicio específico a un portador con cierta calidad de servicio (QoS). A este respecto, se considera que un portador es un contexto o vía de transmisión de información de características definidas; por ejemplo, capacidad, retardo y/o tasa de error binario. Normalmente, se establecerán varios portadores entre una pasarela de una red de comunicaciones móviles y un equipo de usuario; por ejemplo, un teléfono móvil u otro tipo de terminal móvil. Un portador puede transportar tráficos de datos de enlace descendente (DL) en la dirección de la red al equipo de usuario, y puede transportar tráfico de datos en la dirección de enlace ascendente (UL) del equipo de usuario a la red. En la pasarela y en el equipo de usuario, el tráfico de datos, que incluye múltiples paquetes de datos de IP (IP: “Protocolo de Internet”), puede ser filtrado usando filtros de paquetes de tuplas de 5 elementos de IP, dirigiendo con ello los paquetes de datos de IP a un portador deseado.

Específicamente, se desea dirigir tráfico de datos relativo a un servicio específico, por ejemplo, TV móvil, a un portador que ofrezca cierto QoS. Con este fin, el tráfico de datos de DL puede ser sometido a una inspección de paquetes para identificar paquetes de datos relativos a un servicio específico. Cuando se detectan paquetes de datos de un servicio predefinido, esto puede ser indicado mediante señales a un controlador de directrices. El controlador de directrices puede generar entonces correspondientes filtros de paquetes y señalizar estos filtros de paquetes a la pasarela. A continuación, la pasarela usa los filtros de paquetes recibidos para encaminar los paquetes de datos a un portador deseado. Normalmente, el portador tiene una clase de QoS que fue elegida por la empresa explotadora de la red para el servicio específico. En este procedimiento, también puede haber señalización al equipo de usuario; por ejemplo, para establecer el portador e indicar al equipo de usuario filtros de paquetes de UL, que deberían ser usados para encaminar tráfico de datos de UL al portador.

Sin embargo, la solución conocida puede tener problemas, porque, frecuentemente, un servicio puede abrir o cerrar flujos de paquetes IP asociados con el mismo servicio, como hacen, por ejemplo, ciertas aplicaciones de compartición de ficheros entre dispositivos del mismo nivel. En este caso, el resultado sería una señalización exhaustiva para establecer los filtros de paquetes para encaminar los paquetes de datos al portador deseado. Además, el encaminamiento de tráfico de datos de DL usando filtros de paquetes basados en tuplas de 5 elementos de IP requiere recursos de procesamiento significativos en la pasarela. Además, en algunos casos puede ser difícil o imposible que una función de inspección de paquetes describa suficientemente los flujos de paquetes IP asociados con un servicio específico y que indique esto mediante señales al controlador de directrices. Esto puede ocurrir, por ejemplo, si los flujos de paquetes IP están cifrados o si el servicio está asociado con un gran número de flujos de paquetes IP; por ejemplo, en el caso de ciertas aplicaciones de compartición de ficheros entre dispositivos del mismo nivel.

En consecuencia, existe la necesidad de técnicas potentes y eficaces para la gestión del tráfico de red que permitan asignar al tráfico de datos de un servicio específico un nivel deseado de QoS.

En el documento US 2007/0081499 A1, se describe que un filtro de paquetes que ha de ser aplicado por un terminal móvil para filtrar el tráfico de datos de UL puede ser generado para que tenga una característica que está reflejada con respecto a un filtro de paquetes que ha de ser aplicado en un nodo de pasarela para filtrar el tráfico de datos de DL.

El uso de filtros de paquetes para dirigir paquetes de datos a portadores entre un equipo de usuario y la red también se describe en los documentos WO 2007/079773 A1, WO 2007/087828 A1 y la especificación técnica de 3GPP 23.203 V7.5.0 (2007-12).

Compendio

La presente invención se define en las reivindicaciones independientes adjuntas a las que se puede hacer referencia. Las características ventajosas se exponen en las reivindicaciones dependientes adjuntas

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente un entorno de comunicaciones móviles en el que pueden aplicarse conceptos de acuerdo con las realizaciones de la invención para la gestión de tráfico de datos de DL.

La Figura 2 ilustra esquemáticamente un ejemplo de un paquete de datos usado en una realización de la invención.

La Figura 3 ilustra esquemáticamente un ejemplo adicional de un paquete de datos usado en una realización de la invención.

La Figura 4 ilustra esquemáticamente un campo de información en una sección de cabecera de los paquetes de datos.

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

La Figura 6 ilustra esquemáticamente un entorno de comunicaciones móviles en el que pueden aplicarse, para la gestión de tráfico de datos de UL, conceptos según realizaciones de la presente invención.

La Figura 7 ilustra esquemáticamente un identificador y un identificador complementario en los paquetes de datos.

La Figura 8 muestra un diagrama de flujo para ilustrar un método de gestión de tráfico de datos de UL según una realización de la invención.

Descripción detallada de realizaciones

En lo que sigue, la invención será explicada con mayor detalle con referencia a realizaciones ejemplares y a los dibujos adjuntos. Las realizaciones ilustradas están relacionadas con la gestión de tráfico de datos en una red de comunicaciones móviles; por ejemplo, según las especificaciones del 3GPP (Proyecto de Asociación de Tercera Generación). Sin embargo, ha de entenderse que los conceptos descritos en la presente memoria también pueden ser aplicados a otros tipos de redes de comunicaciones. En conexión con las Figuras 1-5, se describirán conceptos de gestión de tráfico de datos de DL; es decir, hacia un equipo de usuario. En conexión con las Figuras 6-8, se describirán conceptos para la gestión de tráfico de datos de UL; es decir, procedente de un equipo de usuario. Así, los conceptos de gestión de tráfico de datos de DL y los conceptos de gestión de tráfico de datos de UL serán descritos por separado. No obstante, ha de entenderse que estos conceptos pueden ser aplicados por separado o en combinación.

La Figura 1 ilustra esquemáticamente un entorno de comunicaciones móviles en las que el tráfico de datos de DL se gestiona de acuerdo con una realización de la invención.

El entorno de red incluye un equipo 10 de usuario, que también puede ser denominado terminal, y varios componentes 22, 24, 26, 30, 100 de red. Entre estos componentes de red hay una red 22 de acceso por radio (RAN). La RAN está basada en cierto tipo o ciertos tipos de tecnología de acceso por radio; por ejemplo, GSM (sistema global para comunicaciones móviles), EDGE (tasa de datos mejorada para la evolución del GSM) o UMTS (sistema universal de telecomunicaciones móviles). Aunque la RAN 22 es ilustrada como un único nodo, ha de entenderse que la RAN 22 puede estar formada, en realidad, por varios componentes, que no son explicados adicionalmente en la presente memoria. La RAN 22 está acoplada a un nodo 24 de transporte, el cual, a su vez, está acoplado a una pasarela 26. Aquí, ha de entenderse que, alternativamente, puede haber más de un nodo 24 de transporte acoplado entre la RAN 22 y la pasarela 26, o que la RAN 22 puede estar directamente acoplada a la pasarela 26. La pasarela 26 puede ser un nodo de soporte pasarela de GPRS (GGSN) que proporcione una conexión de servicios basados en GPRS (GPRS: servicio general de radiotransmisión por paquetes) a una o más redes externas de paquetes de datos. La pasarela 26 también puede ser una pasarela de evolución de arquitectura de sistema (SAE GW) según las especificaciones 3GPP.

Además, la red de comunicaciones móviles incluye un controlador 30 de directrices, que es implementado como una función de reglas de directrices y facturación (PCRF) según las especificaciones 3GPP, y un inspector 100 de paquetes. El controlador de directrices puede ser implementado por soporte físico dedicado o como una función de soporte lógico ejecutada por un procesador. El inspector 100 de paquetes puede ser implementado por soporte físico dedicado o como una función de soporte lógico ejecutada por un procesador. El inspector 100 de paquetes puede ser configurado para implementar una inspección profunda de paquetes (DPI), que puede basarse en examinar tanto una sección de cabecera como una sección de datos de un paquete de datos. Además, la inspección también puede basarse en la recogida de medidas heurísticas, tales como el tiempo entre llegadas de paquetes, los patrones de envío y el tamaño de los paquetes. Tal heurística puede ser aplicada incluso en caso de cifrado. Las secciones de cabecera y las secciones de datos pueden ser examinadas en diferentes capas de protocolo; por ejemplo, en la capa de aplicaciones o en capas inferiores, para identificar diferentes servicios y protocolos. La inspección también se puede realizar con respecto a señalización de control relativa a sesiones. Sin embargo, también pueden implementarse otros tipos de procesos de inspección de paquetes; por ejemplo, basados meramente en una inspección de una sección de cabecera.

Normalmente, la pasarela 26, el controlador 30 de directrices y el inspector 100 de paquetes son considerados componentes de una red central.

El controlador 30 de directrices se comunica con el inspector 100 de paquetes a través de una vía 5 de señalización. La vía 5 de señalización puede ser implementada usando la interfaz Rx o la interfaz Gx según las especificaciones

3GPP. Además, el controlador 30 de directrices se comunica con la pasarela 26 a través de una vía 6 de señalización, que puede ser implementada usando la interfaz Gx según las especificaciones 3GPP.

El controlador 30 de directrices está acoplado, además, a una base de datos 32 de abono y a una base de datos 34 de directrices de servicio a través de una vía 8 de señalización, implementada, por ejemplo, usando una interfaz Sp según las especificaciones 3GPP. Así, el controlador 30 de directrices puede recibir datos de directrices relativos a un usuario específico y/o relativos a un servicio específico disponible en la red de comunicaciones móviles; por ejemplo, TV móvil.

Así, el controlador 30 de directrices proporciona interfaces para soportar las vías 5, 6, 8 de señalización.

Según se ilustra también, el tráfico de datos relativo a servicios entre la red y el equipo 10 de usuario es transportado por varios portadores 52, 54. Normalmente, el tráfico de datos relativo a servicios pertenece a una o más aplicaciones cliente/de dispositivo de igual nivel 12 que se ejecutan en el equipo 10 de usuario. Los portadores 52, 54 se establecen entre el equipo 10 de usuario y la pasarela 26. Los portadores 52, 54 transportan un tráfico de datos tanto en la dirección de DL como en la dirección de UL; es decir, también se puede considerar que están formados de un portador de DL y un portador de UL. Para soportar la comunicación bidireccional en los portadores 52, 54, el equipo 10 de usuario está dotado de una estructura transceptora; es decir, tanto de un receptor 14 para recibir paquetes de datos entrantes procedentes de los portadores 52, 54, como de un transmisor 16 para enviar paquetes de datos salientes por los portadores 52, 54. Los portadores 52, 54 pueden incluir un portador por defecto, generalmente establecido para ofrecer servicios basados en paquetes al equipo 10 de usuario y a uno o más portadores dedicados 54 que pueden tener diferente nivel de QoS, por ejemplo, un nivel mayor de QoS, que el portador por defecto. Cada portador 52, 54 puede estar asociado con un correspondiente perfil de QoS. Los parámetros del perfil de QoS pueden ser un identificador de clase de QoS (QCI), una prioridad de asignación/retención (ARP), una velocidad máxima de transferencia de bits (MBR) y/o una velocidad garantizada de transferencia de bits (GBR). En consecuencia, cada portador 52, 54 puede estar asociado con una correspondiente clase de QoS.

En el equipo 10 de usuario, los paquetes de datos son encaminados a un portador deseado 52, 54 usando filtros 62, 64 de paquetes de UL configurados en correspondencia. En la pasarela 26, los paquetes de datos son encaminados a los portadores deseados 52, 54 usando filtros 72, 74 de paquetes de DL configurados en correspondencia. Los parámetros del perfil de QoS pueden ser señalizados desde el controlador 30 de directrices a la pasarela 26 usando la vía 6 de señalización. De forma similar, los filtros 72, 74 de paquetes de DL que han de usarse en la pasarela 26 pueden ser señalizados desde el controlador 30 de directrices a la pasarela 26 a través de la vía 6 de señalización. En cuanto a los filtros 62, 64 de paquetes de UL usados en el equipo 10 de usuario, estos pueden ser señalizados desde el controlador 30 de directrices a través de la pasarela 26. Sin embargo, en algunas realizaciones, según se explica adicionalmente en conexión con las Figuras 6-8, los filtros 62, 64 de paquetes de UL también pueden ser generados en respuesta al tráfico de datos recibido en el equipo 10 de usuario.

En la red de comunicaciones móviles ilustrada en la Figura 1, el tráfico de datos de DL del equipo 10 de usuario pasa por el inspector 100 de paquetes antes de ser recibido por la pasarela 26. El inspector 100 de paquetes identifica paquetes de datos pertenecientes a uno o más servicios predefinidos y/o pertenecientes a un usuario específico. Esto se puede lograr en función de los datos de control de inspección de paquetes recibidos del controlador 30 de directrices. Si se identifican paquetes de datos pertenecientes a un servicio predefinido específico, el inspector 100 de paquetes proporciona una respectiva indicación al controlador 30 de directrices enviando datos de inspección de paquetes. Además, el inspector 100 de paquetes incluye una función 120 de marcado, que incluye un identificador al paquete de datos inspeccionado. La función 120 de marcado puede ser implementada mediante soporte físico dedicado o como una función de soporte lógico que se ejecute en un procesador. El identificador se selecciona según el servicio identificado al que pertenece el paquete de datos. Por ejemplo, los paquetes de datos que pertenecen a cierto servicio de compartición de ficheros pueden recibir un primer identificador, y los paquetes de datos pertenecientes a cierto servicio de transmisión pueden ser dotados con un segundo identificador. Así, la inclusión del identificador en los paquetes de datos, o el marcado de los paquetes de datos, se logra en función del resultado de una inspección de paquetes o puede incluso formar parte del procedimiento de inspección de paquetes. El identificador puede ser incluido en los paquetes de datos configurando un campo de información en una sección de cabecera del paquete de datos; por ejemplo, punto de código de servicios diferenciados (DSCP). La correlación de un servicio específico con un correspondiente identificador puede ser controlada dinámicamente por el controlador 30 de directrices usando los datos de control de inspección de paquetes. De esta manera, la correlación entre un servicio específico y un correspondiente identificador puede ser controlada dinámicamente en función de datos de directrices. Por ejemplo, la correlación podría variar dependiendo de la hora del día o del día de la semana.

En función de los datos de inspección de paquetes recibidos del inspector 100 de paquetes y en función de los datos de directrices, el controlador 30 de directrices controla la selección y/o la configuración de los filtros 72, 74 de paquetes de DL usados en la pasarela 26 para encaminar los paquetes de datos a los portadores deseados 52, 54. Con este fin, el controlador 30 de directrices incluye un generador 35 de filtros. El generador de filtros puede ser implementado por soporte físico dedicado o como una función de soporte lógico ejecutada por un procesador. El generador 35 de filtros puede construir los filtros de paquetes de DL, seleccionar de una lista filtros preconfigurados de paquetes de DL, y/o configurar filtros seleccionados de paquetes de DL. Los filtros 72, 74 de paquetes de DL

filtran el tráfico de datos de DL en función del identificador que es incluido en los paquetes de datos por el inspector 100 de paquetes. Esto permite un proceso de filtrado sumamente eficaz y fiable, dado que los filtros 72, 74 de paquetes de DL meramente precisan tener en cuenta el identificador incluido por el inspector 100 de paquetes. Por ejemplo, si el identificador es un DSCP en la sección de cabecera de los paquetes de datos, los filtros 72, 74 de paquetes de DL meramente precisan analizar el campo de información DSCP en la sección de cabecera de los paquetes de datos. De esta manera, el tráfico de datos perteneciente a un servicio específico puede ser encaminado dinámicamente a un portador deseado 52, 54 con una correspondiente clase de QoS.

En lo que sigue, se explicarán con mayor detalle conceptos de marcado de paquetes de datos inspeccionados con referencia a tipos ejemplares de paquetes de datos.

La Figura 2 ilustra esquemáticamente paquetes de datos de IP de la versión de IP de tipo 4. Según se ilustra, una sección de cabecera de los paquetes de datos incluye varios campos de información, a los que se denomina “Versión”, “IHL (longitud de cabecera IP)”, “Servicios diferenciados”, “Longitud total”, “Identificación”, “Banderas”, “Desplazamiento del fragmento”, “Tiempo restante de vida”, “Protocolo”, “Suma de comprobación de la cabecera” “Dirección de origen”, “Dirección de destino”, “Opciones” y “Relleno”. En la especificación RFC 791 se definen detalles relativos a estos campos. El campo de información denominado “Servicios diferenciados” está definido en la especificación RFC 2475. Además, la sección de cabecera de un paquete de datos IP también incluirá campos de información que se denominan “Puerto de origen” y “Puerto de destino”. Definen campos de información correspondientes, por ejemplo, el protocolo de control de transporte (TCP), definido en la especificación RFC 793, y el protocolo de datagramas de usuario (UDP), definido por la especificación RFC 768.

Tras la sección de cabecera, los paquetes de datos de IP están normalmente dotados de una sección de datos, en la que pueden incluirse diferentes tipos de tráfico de datos de carga útil.

La Figura 3 ilustra esquemáticamente paquetes de datos de IP según la versión de IP de tipo 6. De nuevo, la sección de cabecera incluye varios campos de información, que se denominan “Versión”, “Servicios diferenciados”, “Etiqueta del flujo”, “Longitud de la carga útil”, “Cabecera siguiente”, “Límite de salto”, “Dirección de origen” y “Dirección de destino”. Esta estructura de la sección de cabecera está definida en la especificación RFC 2460. Además, la sección de cabecera también puede comprender campos de información denominados “Puerto de origen” y “Puerto de destino”, según define, por ejemplo, el TCP o el UDP. De nuevo, la sección de cabecera estará seguida normalmente por una sección de datos que puede transportar tipos diversos de datos de carga útil.

Para los fines de la presente divulgación, solo los campos de información denominados “Servicios diferenciados”, “Dirección de origen”, “Dirección de destino”, “Puerto de origen” y “Puerto de destino” serán objeto de exposición adicional. En lo referente a otros campos de información, pueden obtenerse explicaciones adicionales de las especificaciones de RFC anteriormente mencionadas.

El campo de información “Dirección de origen” indica la dirección IP en la que se origina un paquete de datos. De modo similar, el campo de información “Dirección de destino” indica la dirección IP a la que está destinado el paquete de datos. En la versión 4 de IP, la dirección de origen y la dirección de destino son valores de 32 bits. En la versión 6 de IP, 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 función de la dirección de origen, de la dirección de destino, del puerto de origen y del puerto de destino, un flujo de paquetes IP puede ser definido como un flujo de paquetes IP entre un primer punto terminal definido por la dirección de origen y el puerto de origen, y un segundo punto terminal 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 también se denomina “tupla de 5 elementos de IP”.

El campo de información “Servicios diferenciados” está incluido tanto en los paquetes de datos de la versión 4 de IP como en los paquetes de datos de la versión 6 de IP. Según 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 está ilustrada esquemáticamente en la Figura 4.

Según se ilustra en la Figura 4, se usan seis bits del campo de información, es decir, los bits 0-5, para definir el punto de código de servicios diferenciados (DSCP). Los otros dos bits no son utilizados. Usando el DSCP puede controlarse el envío de los paquetes de datos por los nodos de red. Para paquetes de datos pertenecientes a diferentes tipos de servicios, pueden seleccionarse procedimientos de envío diferentes. Los DSCP pueden estar estandarizados. Además, hay disponible una gama de DSCP no estandarizados.

En lo que sigue se describirá con mayor detalle un procedimiento de gestión del tráfico de datos de DL de acuerdo con una realización de la invención. Esto se logrará haciendo referencia a el entorno de red de comunicaciones móviles ilustrado en la Figura 1.

Según se ha mencionado anteriormente, la red de comunicaciones móviles puede soportar varias clases de QoS asociadas con diferentes portadores. Las clases de QoS pueden ser identificadas por un correspondiente QCI. Para marcar paquetes identificados de datos de un servicio específico en el inspector 100 de paquetes, se define un DSCP dedicado; por ejemplo, de la gama de DSCP no estandarizados. En consecuencia, puede haber un DSCP dedicado para cada portador.

Además, se define una tabla de correlaciones que correlaciona con un DSCP dedicado cada servicio que ha de ser detectado por el inspector 100 de paquetes. Así, pueden usarse diferentes DSCP dedicados para marcar paquetes de datos pertenecientes a servicios diferentes. Sin embargo, también es posible que paquetes de datos de diferentes servicios sean marcados con el mismo DSCP; por ejemplo, si estos servicios hubieran de ser asignados a la misma clase de QoS. Esta tabla de correlaciones puede ser mantenida por el controlador 30 de directrices y comunicada ulteriormente al inspector 100 de paquetes, usando, por ejemplo, la vía 5 de señalización. Alternativamente, el inspector 100 de paquetes también puede estar configurado estadísticamente con la tabla de correlaciones. Si la tabla de correlación en el inspector 100 de paquetes es dinámicamente configurable por el controlador 30 de directrices, también es posible reconfigurar la tabla de correlaciones en función de datos de directrices. Por ejemplo, la tabla de correlaciones podría ser reconfigurada dependiendo de la hora del día o dependiendo del día de la semana.

Si el inspector 100 de paquetes detecta un flujo de paquetes IP perteneciente a un servicio predefinido, esto es señalizado al controlador 30 de directrices en los datos de inspección de paquetes. Además, la función 120 de marcado del inspector 100 de paquetes marca los paquetes de datos perteneciente al servicio con el DSCP según se define en la tabla de correlaciones. Para otros paquetes de datos, es decir, paquetes de datos que no tienen la identificación de pertenecer a un servicio predefinido, se puede configurar un DSCP por defecto. Por ejemplo, el DSCP por defecto puede ser cero. Como alternativa, la configuración de un DSCP puede ser omitida para paquetes de datos que no tienen la identificación de pertenecer a un servicio predefinido. En los datos de inspección de paquetes, el inspector 100 de paquetes también puede señalizar al controlador 30 de directrices un identificador de servicio. Por medio del identificador de servicio, el servicio identificado y/o el DSCP usado para marcar los correspondientes paquetes de datos pueden ser señalizados al controlador 30 de directrices. Se puede seleccionar de forma apropiada el desencadenamiento de señalización basado en la frecuencia o los sucesos hacia el controlador 30 de directrices.

En respuesta los datos de inspección de paquetes, el controlador 30 de directrices determina un filtro de paquetes de DL que opera en función del DSCP usado para marcar los paquetes de datos del servicio identificado. Según una realización, el filtro de paquetes de DL puede operar sustancialmente únicamente en función del DSCP usado para marcar los paquetes de datos. El filtro de paquetes de DL es señalizado a la pasarela 26.

Usando el filtro de paquetes de DL, la pasarela 26 encamina entonces al correspondiente portador 52, 54 los paquetes de datos de DL que están marcados con el DSCP. El portador 52, 54 puede existir ya. Si el portador no existe, puede ser establecido tras recibir la señalización del controlador 30 de directrices. Es decir, si ya está establecido un portador 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 este portador ya existente. Si no existe ningún portador tal, se establecerá un portador de la clase de QoS asociada con el DSCP tras recibir la señalización del filtro de paquetes de DL del controlador 30 de directrices.

La Figura 5 muestra un diagrama de flujo para ilustrar esquemáticamente un método 200 de gestión de tráfico de datos de DL según los conceptos anteriormente mencionados.

En la etapa 210, se reciben datos de inspección de paquetes, por ejemplo, en el controlador 30 de directrices. Los datos recibidos de inspección de paquetes pueden incluir un identificador de servicio que indique un servicio al que pertenecen los paquetes de datos identificados. Además, los datos de inspección de paquetes pueden indicar un identificador que es usado 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 directrices. Los datos de directrices pueden incluir directrices generales definidas por una empresa explotadora de una red de comunicaciones móviles de cómo gestionar paquetes de datos de un servicio específico, o pueden estar relacionados con el usuario; es decir, definen cómo gestionar paquetes de datos de un servicio específico y un usuario específico. Los datos de directrices también pueden distinguir entre diferentes grupos de abonados o pueden definir un cupo de volumen de un usuario, grupo de abonados o servicio. Específicamente, los datos de directrices pueden indicar qué clase de calidad de servicio debería ser dada a los paquetes de datos pertenecientes a un servicio específico. Esta información puede variar dinámicamente, en función, por ejemplo, de la hora del día, del día de la semana o del cupo de volumen usado.

En la etapa 230, se determina un filtro de paquetes de DL en función de los datos de inspección de paquetes y de los datos de directrices. En particular, se determina un filtro de paquetes de DL que opera en función de un identificador incluido en los paquetes de datos en respuesta al procedimiento de inspección de paquetes. El filtro de paquetes de DL es usado entonces para encaminar los paquetes de datos marcados a un portador que tiene la

clase de QoS deseada. Con este fin, el filtro determinado de paquetes de DL puede ser señalizado desde un controlador de directrices, por ejemplo, el controlador 30 de directrices, a una pasarela, por ejemplo, la pasarela 26.

La Figura 6 ilustra esquemáticamente un entorno de comunicaciones móviles en el que el tráfico de datos de UL es gestionado según una realización de la invención. El entorno de comunicaciones móviles de la Figura 6 es en general similar al de la Figura 1, y los componentes similares han sido designados con los mismos números de referencia. Para detalles adicionales, se hace referencia a las correspondientes explicaciones en conexión con la Figura 1.

Según los conceptos ilustrados en la Figura 6, la información de los paquetes de datos de DL es usada en el equipo 10 de usuario para formar reglas locales para encaminar paquetes de datos de UL. Aquí ha de hacerse notar que, en un escenario de comunicaciones móviles, un flujo de paquetes de datos de IP es normalmente bidireccional. Aunque el transporte de datos de carga útil se produzca solo en una dirección, por ejemplo, en función de paquetes TCP, el flujo de paquetes IP también incluirá normalmente paquetes de control, por ejemplo, paquetes TCP de acuse de recibo, transmitidos en la dirección opuesta. Además, las direcciones IP y los números de puerto de origen y destino de un flujo de paquetes IP son normalmente simétricos; es decir, el punto terminal de destino (identificado por una dirección IP y un número de puerto) en una dirección es el mismo que el punto terminal de origen (identificado por una dirección IP y un número de puerto) en la otra dirección, y viceversa. Debido a la simetría, los paquetes del mismo flujo de paquetes IP que fluyen de forma opuesta tendrán identificadores de dirección “complementarios” e identificadores de puerto “complementarios”, lo que significa que el identificador de origen en una dirección es igual que el identificador de destino en la otra dirección.

Según los conceptos de gestión de tráfico de datos de UL explicados en lo que sigue, se supondrá que el tráfico de datos de DL ya está correlacionado con clases de QoS y los correspondientes portadores. Esto puede lograrse según los conceptos explicados anteriormente en conexión con la Figura 1. Es decir, el entorno de comunicaciones móviles de la Figura 6 también podría incluir el inspector 100 de paquetes y las funcionalidades asociadas para la gestión del tráfico de datos de DL, según se ha explicado en conexión con la Figura 1. No obstante, ha de entenderse que también son aplicables otros conceptos de correlación del tráfico de datos de DL con clases de QoS y portadores.

Según se ilustra en la Figura 6, el equipo 10 de usuario incluye, además, una función 220 de gestión especular. La función 220 de gestión especular puede ser implementada mediante soporte físico dedicado o como una función de soporte lógico que se ejecute en un procesador. La función 220 de gestión especular 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, el identificador de un punto terminal de destino, por ejemplo, la dirección IP de destino y/o el puerto de destino, es igual que el identificador de un punto terminal de origen, por ejemplo, la dirección IP de origen y/o el puerto de origen, en el identificador. Cada uno de los identificadores primero y segundo pueden ser la tupla de 5 elementos de IP. La función 220 de gestión especular controla los filtros 62, 64 de paquetes de UL, que están basados en tuplas de 5 elementos de IP, de tal modo que los paquetes de datos salientes que tengan el segundo identificador complementario sean encaminados al mismo portador del que se recibieron los paquetes de datos entrantes que tenían el primer identificador. De esta manera, no es necesaria ninguna señalización explícita entre la pasarela 26 y el equipo 10 de usuario para seleccionar o configurar los filtros 62, 64 de paquetes de UL. Si la función 220 de gestión especular detecta que se ha correlacionado un nuevo flujo de paquetes IP con un portador 52, 54 o se establece un nuevo portador 52, 54, la función 220 de gestión especular puede generar automáticamente un correspondiente filtro 62, 64 de paquetes UL. Si una tupla específica de 5 elementos de IP identifica paquetes de datos entrantes en la dirección de DL, el filtro 62, 64 de paquetes UL estará configurado para encaminar paquetes de datos salientes que tienen una tupla complementaria de 5 elementos de IP al mismo portador del cual se reciben los paquetes de datos entrantes.

En la Figura 7 se ilustran la estructura de un identificador y un identificador complementario, que están basados en la tupla de 5 elementos de IP. Sin embargo, se debe entender que son asimismo posibles otros tipos de identificadores e identificadores complementarios. En general, el identificador complementario indica la fuente identificada en el identificador de un paquete de datos entrantes como destino de un paquete de datos saliente.

Según se muestra en la Figura 7, un identificador basado en la tupla de 5 elementos 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 son intercambiadas en comparación con el identificador. De forma similar, en el identificador complementario el puerto de origen y el puerto de destino son intercambiados en comparación con el identificador. El identificador de protocolo permanece inalterado. En otras realizaciones, pueden usarse tipos diferentes de identificador e identificador complementario, en función, por ejemplo, de solo parte de la tupla de 5 elementos de IP. Por ejemplo, en el identificador complementario, solo podrían intercambiarse la dirección de origen y la dirección de destino en comparación con el identificador.

En lo que sigue, se explicará con mayor detalle un procedimiento de gestión de paquetes de datos de UL según una realización de la invención con referencia a las estructuras mostradas en la Figura 6.

Inicialmente, los paquetes de datos de UL relativos a un servicio específico pueden ser transmitidos del equipo 10 de usuario a la pasarela 26 por un portador arbitrario; por ejemplo, por el portador por defecto. Entonces, el correspondiente flujo de paquetes IP también incluirá paquetes de datos transmitidos en la dirección de DL. Estos paquetes de datos serán correlacionados con una clase deseada de QoS y el correspondiente portador 52, 54, usando, por ejemplo, los conceptos explicados en conexión con la Figura 1. Este procedimiento también puede implicar el establecimiento de un nuevo portador asociado con la clase deseada de QoS.

La función 220 de gestión especular en el equipo 10 de usuario detecta entonces los paquetes de datos entrantes que se reciben de este portador 52, 54 y genera un filtro 62, 64 de paquetes UL “reflejado”, que opera en función de una tupla de 5 elementos de IP que es complementaria de una tupla de 5 elementos de IP en los paquetes de datos entrantes recibidos. Ha de entenderse aquí que puede haber presentes diferentes flujos de paquetes IP en un solo portador 52, 54 y que múltiples filtros 62, 64 de paquetes de UL pueden encaminar paquetes de datos salientes al mismo portador 52, 54. Si hay un nuevo flujo de paquetes IP con paquetes de datos entrantes en un portador 52, 54 o se establece un nuevo portador, se generará un correspondiente nuevo filtro 62, 64 de paquetes de datos de UL.

Cuando se aplican los conceptos anteriormente mencionados, el equipo 10 de usuario puede estar dotado de una funcionalidad para indicar a la red de comunicaciones móviles que soporta la función 220 de gestión especular. Por ejemplo, esta podría estar incluida en la señalización de gestión de sesiones; por ejemplo, durante un procedimiento de conexión entre el equipo 10 de usuario y la red central. A título de ejemplo, podría añadirse un elemento de información al procedimiento de señalización en el que el equipo 10 de usuario pueda indicar que soporta la función 220 de gestión especular. La Figura 6 ilustra esquemáticamente una correspondiente vía 2 de señales que se extiende desde el equipo 10 de usuario. Ha de entenderse aquí que se representa esquemáticamente que la vía 2 de señalización se extiende desde el equipo 10 de usuario directamente hasta un nodo específico de red, por ejemplo, según se ilustra, al controlador 30 de directrices, pero normalmente puede ser implementada a través de otros nodos de red. Por ejemplo, en una red UMTS de comunicaciones, la vía 2 de señalización podría extenderse desde el equipo 10 de usuario hasta un nodo de soporte servidor de GPRS (SGSN). En una red de comunicaciones de evolución a largo plazo/evolución de arquitectura de servicio (SAE/LTE), la vía 2 de señalización podría extenderse del equipo 10 de usuario a una entidad de gestión de la movilidad (MME). A continuación, desde estos nodos de red, la información de señalización puede ser enviada o distribuida a otros nodos de red; por ejemplo, al controlador 30 de directrices.

En algunas realizaciones, la información de que el equipo 10 de usuario soporta la función 220 de gestión especular también puede ser distribuida entre los nodos de la red central, por ejemplo, al controlador 30 de directrices o a un nodo que soporte una función de inspección de paquetes; por ejemplo, el inspector 100 de paquetes mostrado en la Figura 1. Con este fin, puede reutilizarse la interfaz Gx o la interfaz Rx según las especificaciones 3GPP.

Según algunas realizaciones, puede proporcionarse una vía 4 de señalización adicional desde la red de comunicaciones móviles hasta el equipo 10 de usuario. Usando esta vía 4 de señalización, puede ser posible activar o desactivar la función 220 de gestión especular portador por portador. Esto puede ser útil si no todas las aplicaciones o los servicios requieren esta función para ser activados. Por ejemplo, en algunos casos la tupla de 5 elementos de IP en paquetes de datos de un servicio se puede definir estáticamente y puede usarse un correspondiente filtro estático 62, 64 de paquetes UL en el equipo 10 de usuario. De nuevo, ha de entenderse que se representa esquemáticamente que la vía 4 de señalización se extiende hasta el equipo 10 de usuario directamente desde un modo específico de red, por ejemplo, según se ilustra, desde el controlador 30 de directrices, pero normalmente puede ser implementada a través de otros nodos de red. Por ejemplo, en una red UMTS de comunicaciones, la vía 2 de señalización podría extenderse desde un nodo de soporte servidor de GPRS (SGSN) hasta el equipo 10 de usuario. En una red de comunicaciones de evolución a largo plazo/evolución de arquitectura de servicio (SAE/LTE), la vía 2 de señalización podría extenderse de una entidad de gestión de la movilidad (MME) al equipo 10 de usuario. A su vez, estos nodos de red pueden recibir la información de señalización desde otros nodos de red; por ejemplo, del controlador 30 de directrices.

En algunas realizaciones, la red de comunicaciones móviles puede indicar mediante señales al equipo 10 de usuario si debería aplicarse o no la función 220 de gestión especular, usando, por ejemplo, procedimientos estandarizados de establecimiento o modificación de portadores definidos en las especificaciones 3GPP. Con este fin, podría añadirse un correspondiente elemento de información a los procedimientos estandarizados de establecimiento o modificación de portadores. En tales casos, la señalización del equipo 10 de usuario a la red de comunicaciones móviles de que la función 220 de gestión especular está soportada también podría ser implementada portador por portador. Es decir, la correspondiente señalización podría especificar el soporte de la función 220 de gestión especular para un nuevo portador, o podría modificar la información de soporte para un portador ya establecido.

La Figura 8 muestra un diagrama de flujo que ilustra un método 300 para gestionar tráfico de datos de UL según los conceptos anteriormente mencionados.

En la etapa 310, se reciben desde un portador paquetes de datos entrantes con un primer identificador. Según se ha explicado anteriormente, el portador puede estar asociado con una correspondiente clase de QoS, y el primer identificador puede ser una tupla de 5 elementos de IP.

En la etapa 320, se detectan paquetes de datos salientes con un segundo identificador complementario. Esto se puede lograr generando o configurando un filtro de paquetes UL “reflejado” que opera en función de una tupla de 5 elementos de IP que es complementaria de la tupla de 5 elementos de IP en los paquetes de datos entrantes recibidos del portador.

En la etapa 330, se encaminan los paquetes de datos salientes con el segundo identificador al mismo portador desde el que se reciben los paquetes de datos entrantes con el primer identificador. De nuevo, esto se puede lograr seleccionando o configurado un correspondiente filtro de paquetes UL “reflejado” que opere, por ejemplo, en función del identificador complementario o una parte del mismo.

Según los conceptos explicados anteriormente, es posible correlacionar dinámicamente el tráfico de datos relacionado con un servicio con una clase deseada de QoS en función, por ejemplo, de datos de directrices específicos al usuario y/o en función de datos de directrices específicos al servicio. Además, la correlación podría depender de la hora del día, del día de la semana o de otros parámetros. Así, pueden definirse diversas directrices diferentes en los datos de directrices para controlar la correlación entre el tráfico de datos relativo a servicios y una clase de QoS. Una directriz tal puede ser incluso para bloquear el tráfico de datos relativo a un servicio específico en la pasarela.

Además, el control de la QoS en función de los datos de directrices se puede lograr, de manera eficaz, sin requerir señalización excesiva en las interfaces de la red central o con el equipo de usuario. Cuando se combinan los conceptos de gestión del tráfico de datos de DL según se explica en conexión con las Figuras 1-5 con los conceptos de gestión del tráfico de datos de UL según se explica en conexión con las Figuras 6-8, se obtiene una solución eficaz que permite gestionar tanto el tráfico de datos de DL como el tráfico de datos de UL.

Además, los conceptos descritos anteriormente no dependen de establecer portadores que no son necesarios. En vez de ello, pueden establecerse portadores cuando sea necesario, usando por ello de forma eficiente los recursos de red disponibles.

Ha de entenderse que los conceptos explicados anteriormente son meramente ejemplares y susceptibles de diversas modificaciones. Por ejemplo, no es preciso que los nodos de red ilustrados en las Figuras 1 y 6 sean implementados como nodos separados, sino que pueden estar integrados en un único componente de red. Por ejemplo, el inspector 100 de paquetes también podría estar integrado en la pasarela 26. Los conceptos pueden ser aplicados en diversos tipos de redes de comunicaciones móviles. Por último, ha de hacerse notar que la solución para la gestión del tráfico de datos de UL explicada en conexión con las Figuras 6-8 no está limitada a la gestión del tráfico de datos de UL procedente de un equipo de usuario. Más bien, estos conceptos pueden ser aplicados en general a todas las situaciones en las que los paquetes de datos entrantes ya están correlacionados con un portador específico y hay correspondientes paquetes de datos salientes.

REIVINDICACIONES

1. Un método de gestión del tráfico de red, llevado a cabo por un equipo (10) de usuario, que comprende:

- recibir una señal (4) de control que indica activar selectivamente la detección y encaminamiento de paquetes de datos salientes;

- recibir paquetes de datos entrantes de uno de varios portadores (52, 54), incluyendo los paquetes de datos entrantes un primer identificador que indica un origen;

- detectar, si se ha activado selectivamente por la señal (4) de control, los paquetes de datos salientes que incluyen un segundo identificador que indica el origen del primer identificador como destino de los paquetes de datos salientes;

- encaminar los paquetes de datos salientes detectados al mismo portador (52, 54) del que se reciben los paquetes de datos entrantes que tienen dicho primer identificador.

2. El método según la reivindicación 1,

en el que el equipo (10) de usuario detecta un nuevo flujo en los paquetes de datos entrantes recibidos, y detecta los paquetes de datos salientes que incluyen el segundo identificador en respuesta a la detección del nuevo flujo.

3. El método según la reivindicación 1 o 2,

en el que el equipo (10) de usuario, en respuesta a la detección del nuevo flujo, genera un filtro (62, 64) de paquetes que opera en función del segundo identificador.

4. El método según la reivindicación 3,

en el que el equipo (10) de usuario detecta paquetes de datos salientes que incluyen el segundo identificador por medio del filtro (62, 64) de paquetes.

5. El método según la reivindicación 1,

en el que los portadores (52, 54) están asociados cada uno con una correspondiente clase de Calidad de Servicio.

6. El método según una cualquiera de las reivindicaciones precedentes, que comprende:

- indicar a un componente (22, 24, 26, 30, 100) de red que el equipo (10) de usuario soporta la detección y el encaminamiento de los paquetes de datos salientes.

7. El método según una cualquiera de las reivindicaciones precedentes,

en el que los paquetes de datos entrantes incluyen un identificador correlacionado con un servicio específico, estando incluido el identificador en los paquetes de datos entrantes en respuesta a una inspección de paquetes.

8. El método según la reivindicación 7,

en el que el identificador es un campo Punto de Código de Servicios Diferenciados en una sección de cabecera de los paquetes de datos entrantes.

9. Un equipo (10) de usuario, que es capaz de:

- - recibir una señal (4) de control que indica activar selectivamente la detección y encaminamiento de paquetes de datos salientes;

- recibir paquetes de datos entrantes desde uno de varios portadores (52, 54), incluyendo los paquetes de datos entrantes un primer identificador que indica un origen;

- detectar, si se ha activado selectivamente por la señal (4) de control, los paquetes de datos salientes que incluyen un segundo identificador que indica el origen del primer identificador como destino de los paquetes de datos salientes;

- encaminar los paquetes de datos salientes detectados al mismo portador (52, 54) del que se reciben los paquetes de datos entrantes que tienen dicho primer identificador.

10. El equipo (10) de usuario según la reivindicación 9,

estando configurado el equipo (10) de usuario para llevar a cabo las etapas del método según una cualquiera de las reivindicaciones 1-8.

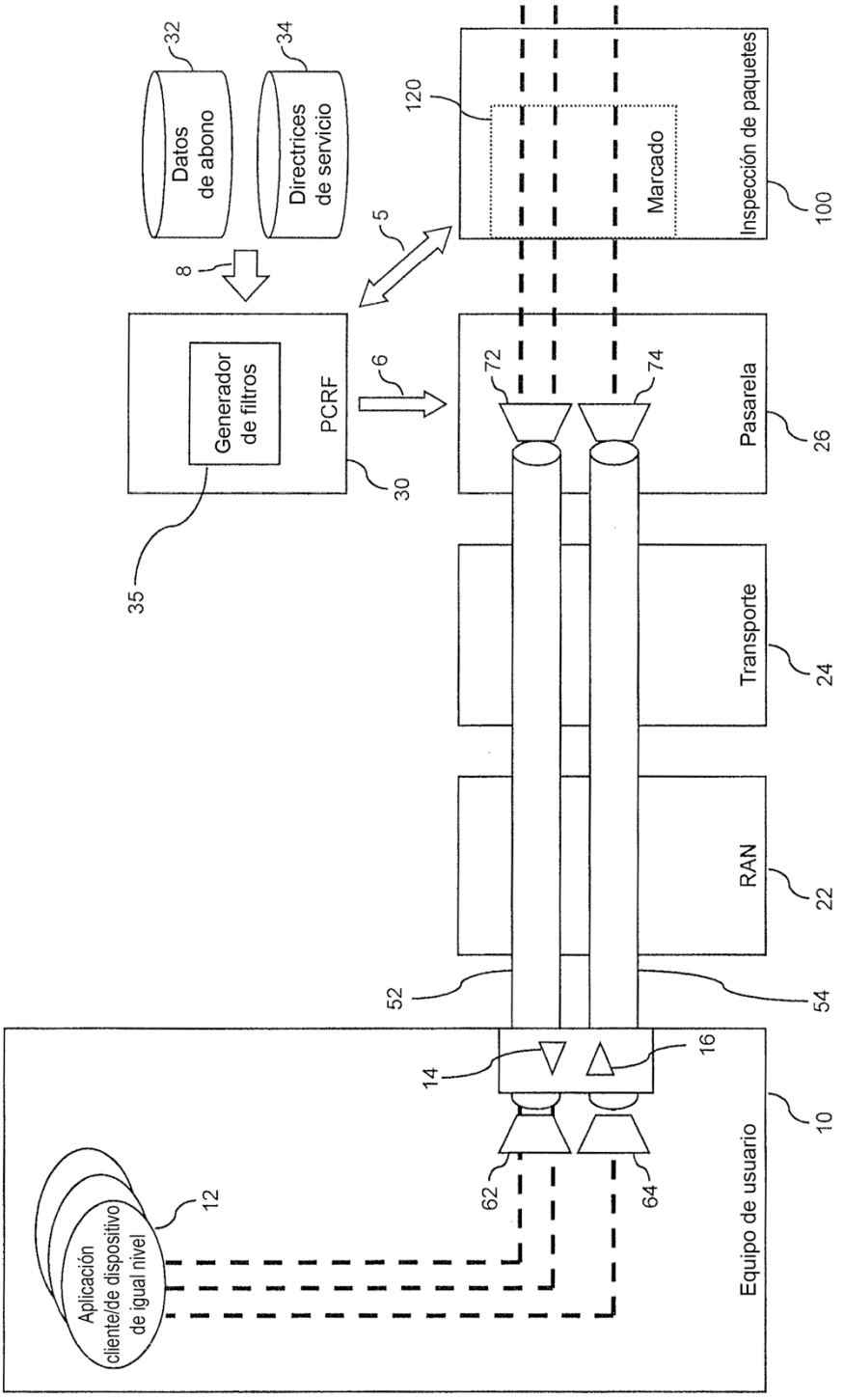
Datos de abono
32
Directrices de servicio
34
8
5
120
Marcado
Inspección de paquetes
100
Generador de filtros
PCRF
30
6
35
72
74
Pasarela
26
Transporte
24
RAN
22
52
54
14
16
62
64
Equipo de usuario
10
Aplicación cliente/de dispositivo de igual nivel
12

FIG. 1

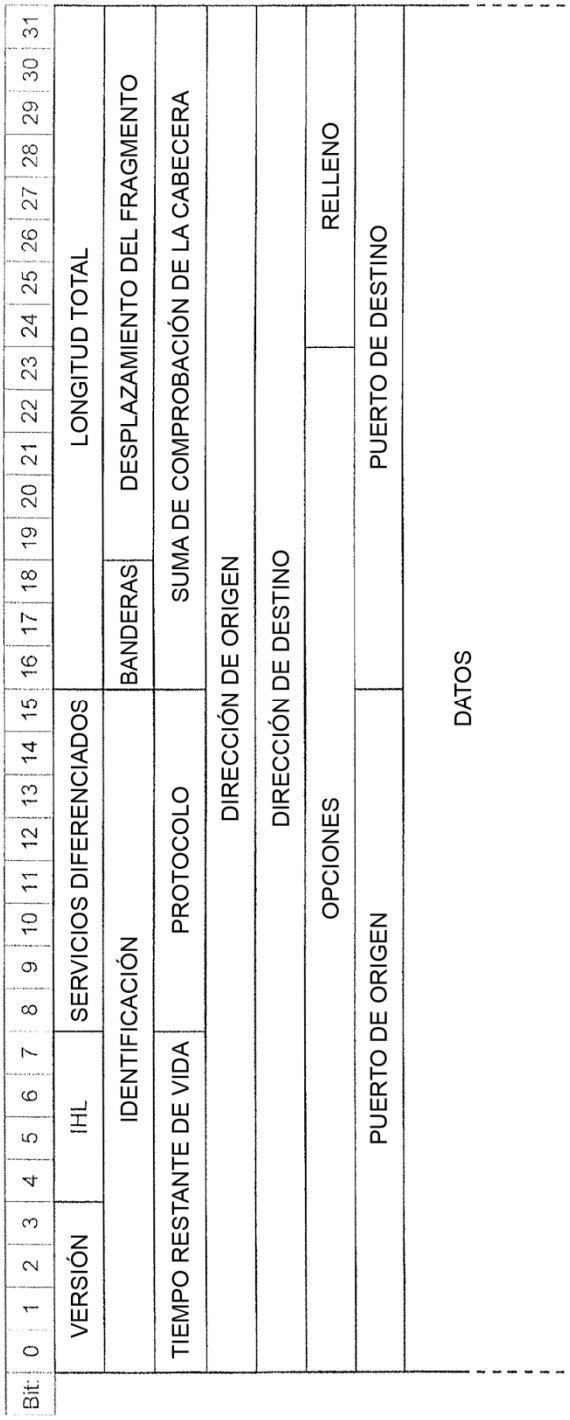
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSIÓN
IHL
SERVICIOS DIFERENCIADOS
LONGITUD TOTAL
IDENTIFICACIÓN
BANDERAS
DESPLAZAMIENTO DEL FRAGMENTO
TIEMPO RESTANTE DE VIDA
PROTOCOLO
SUMA DE COMPROBACIÓN DE LA CABECERA
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO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

FIG. 2

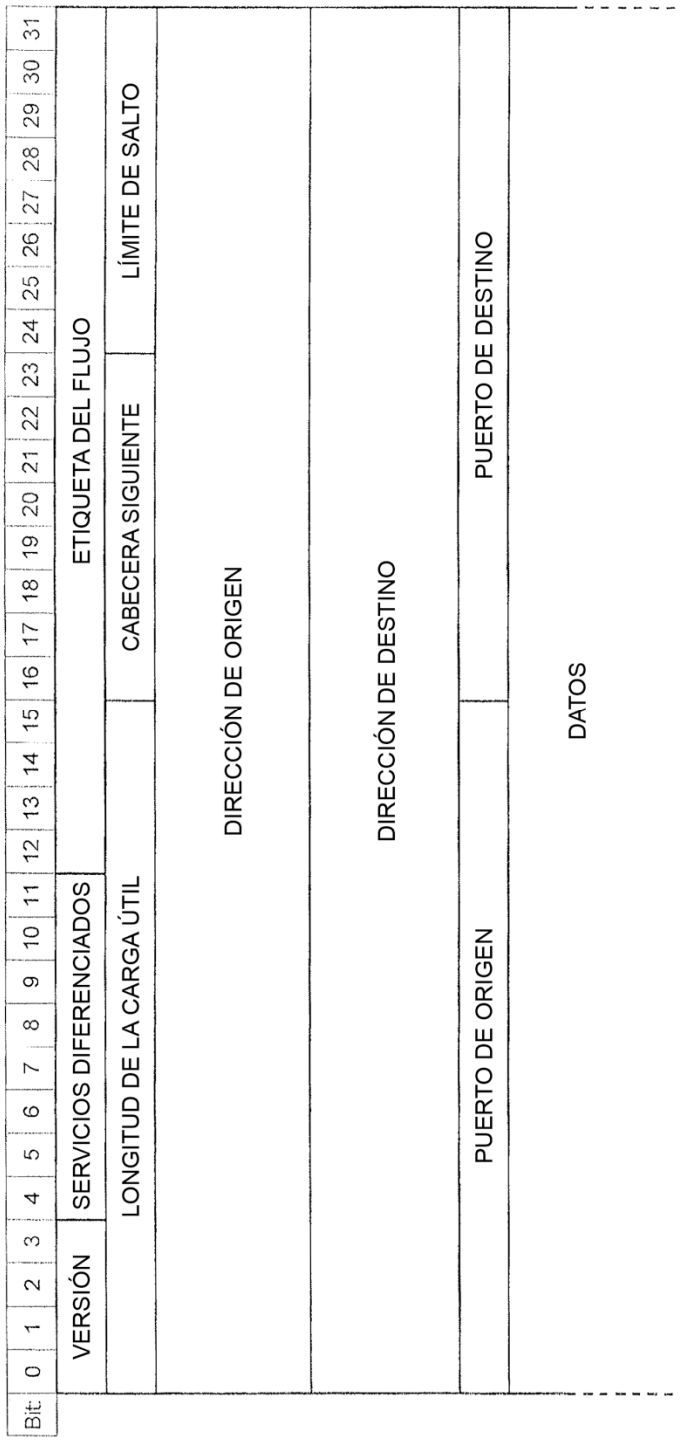
Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VERSIÓN
SERVICIOS DIFERENCIADOS
ETIQUETA DEL FLUJO
LONGITUD DE LA CARGA ÚTIL
CABECERA SIGUIENTE
LÍMITE DE SALTO
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
PUERTO DE ORIGEN
PUERTO DE DESTINO
DATOS

FIG. 3

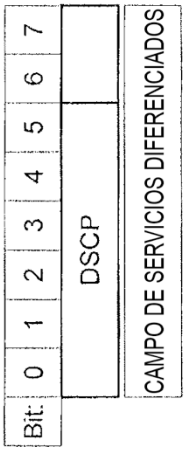

FIG. 4

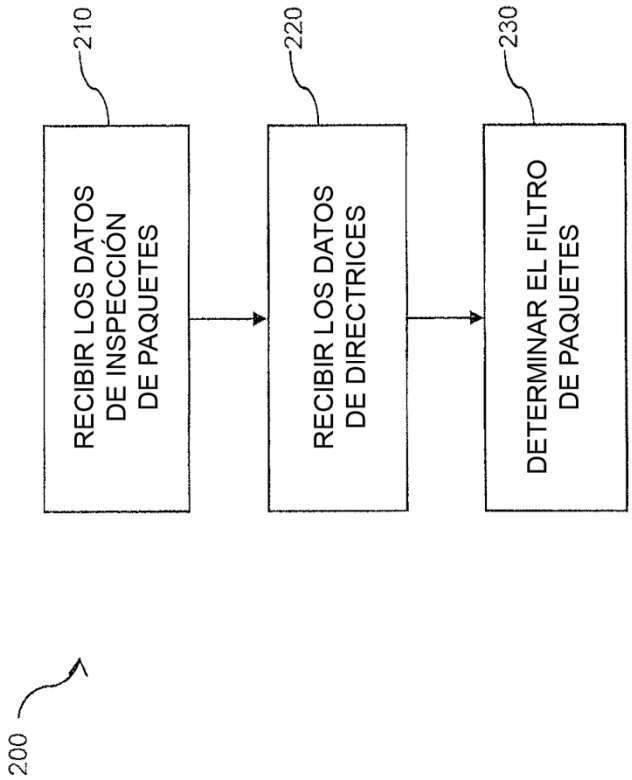
200
210
RECIBIR LOS DATOS DE INSPECCIÓN DE PAQUETES
220
RECIBIR LOS DATOS DE DIRECTRICES
230
DETERMINAR EL FILTRO DE PAQUETES

FIG. 5

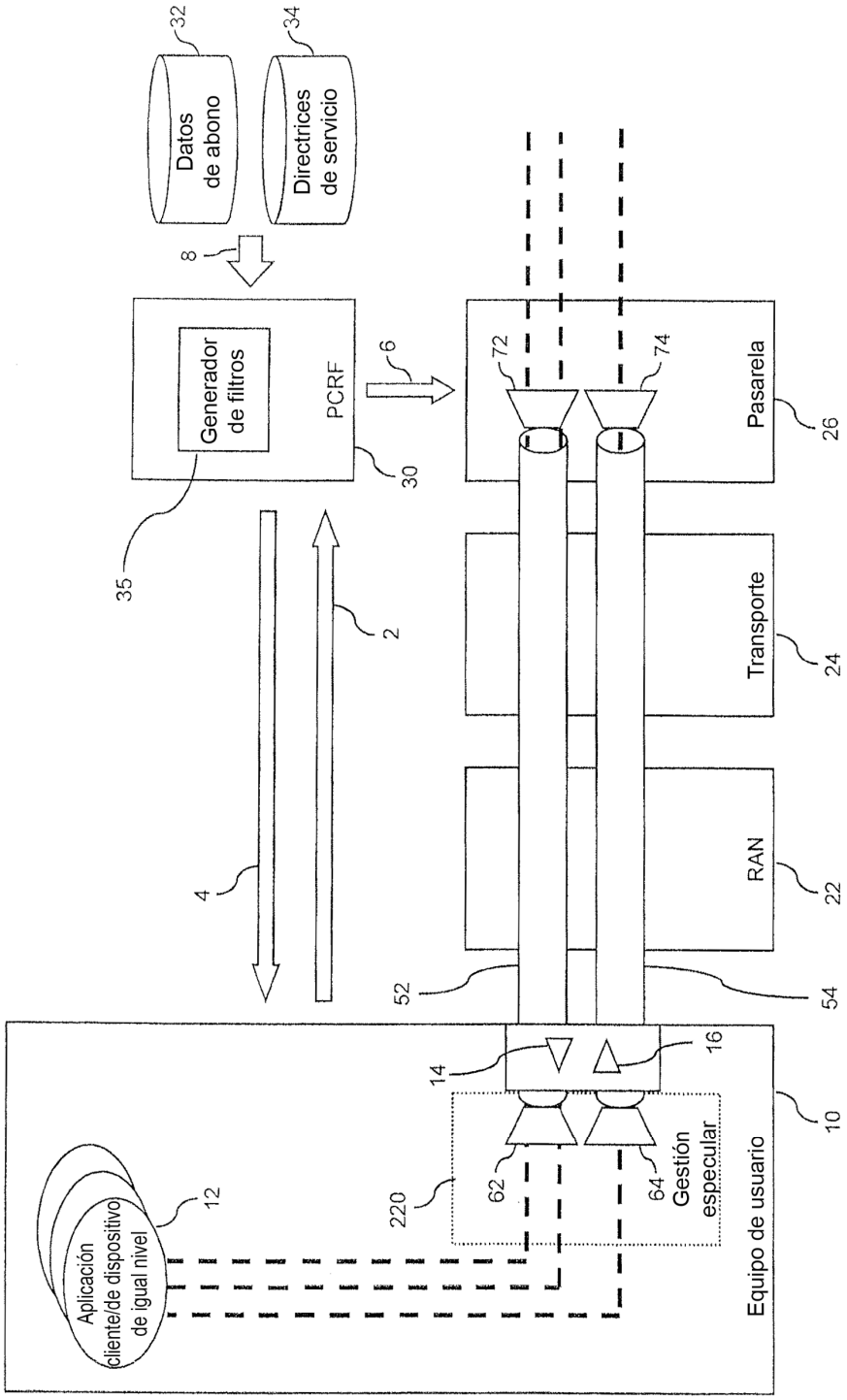
32
Datos de abono
34
Directrices de servicio
8
Generador de filtros
PCRF
6
30
35
2
4
72
74
Pasarela
26
Transporte
24
RAN
22
52
54
14
16
62
64
Gestión especular
220
Aplicación cliente/de dispositivo de igual nivel
12
Equipo de usuario
10

FIG. 6

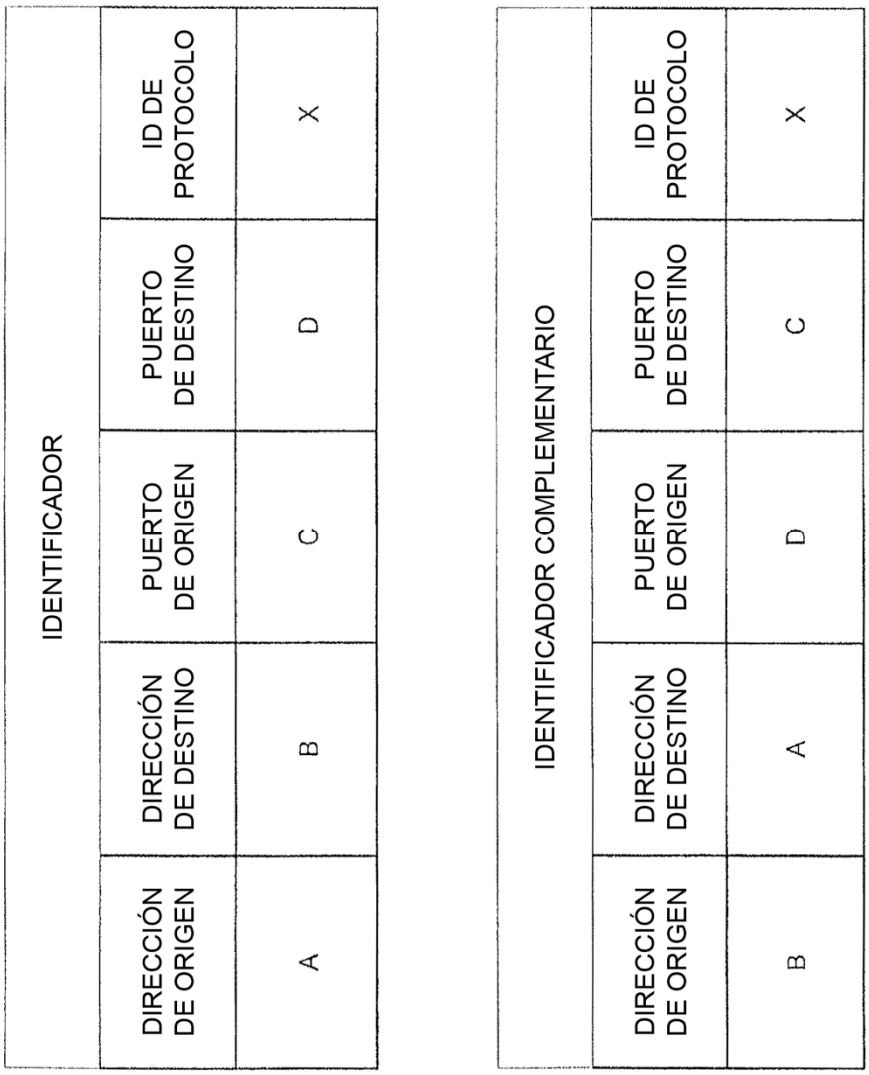
IDENTIFICADOR
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
PUERTO DE ORIGEN
PUERTO DE DESTINO
ID DE PROTOCOLO
A
B
C
D
X
IDENTIFICADOR COMPLEMENTARIO
DIRECCIÓN DE ORIGEN
DIRECCIÓN DE DESTINO
PUERTO DE ORIGEN
PUERTO DE DESTINO
ID DE PROTOCOLO
B
A
D
C
X

FIG. 7

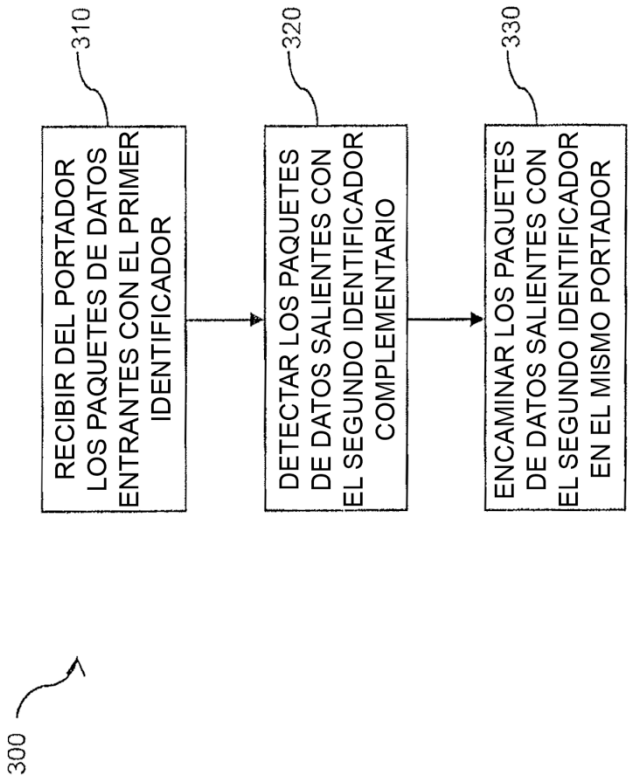
300
310
RECIBIR DEL PORTADOR LOS PAQUETES DE DATOS ENTRANTES CON EL PRIMER IDENTIFICADOR
320
DETECTAR LOS PAQUETES DE DATOS SALIENTES CON EL SEGUNDO IDENTIFICADOR COMPLEMENTARIO
330
ENCAMINAR LOS PAQUETES DE DATOS SALIENTES CON EL SEGUNDO IDENTIFICADOR EN EL MISMO PORTADOR

FIG. 8