(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 291 847**

(51) Int. Cl.:
G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **04704301 .3**
(86) Fecha de presentación : **22.01.2004**
(87) Número de publicación de la solicitud: **1590719**
(87) Fecha de publicación de la solicitud: **02.11.2005**

(54) Título: **Transporte basado en mensajes de información de control de carga.**

(30) Prioridad: **30.01.2003 US 443573 P**
09.12.2003 US 730004

(45) Fecha de publicación de la mención BOPI:
01.03.2008

(45) Fecha de la publicación del folleto de la patente:
01.03.2008

(73) Titular/es: **Nokia Corporation**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Ylä-Outinen, Petteri;**
Latvala, Mikael;
Lahtinen, Lauri;
Tuunanen, Heikki;
Westman, Ilkka y
Höneisen, Bernhard

(74) Agente: **Curell Suñol, Marcelino**

DESCRIPCIÓN

Transporte basado en mensajes de información de control de carga.

Campo de la invención

La presente invención se refiere a un método y un sistema para controlar la carga de procesado en una red de datos por paquetes, tal como un Subsistema Multimedia por Protocolo de Internet (IP) (IMS) proporcionado sobre una red de datos por paquetes para ofrecer servicios de voz y multimedia, por ejemplo, para dispositivos móviles de tercera generación.

Antecedentes de la invención

Se supone que en el futuro casi todas las redes de comunicaciones fijas y móviles se basarán en la tecnología de Internet. Especialmente, las redes futuras estarán lideradas por servicios que combinarán varios tipos y modos de comunicación. La propia voz será simplemente un elemento, aunque importante, en la arquitectura completa de comunicaciones.

El Protocolo de Inicio de Sesión (SIP) tal como se define en la especificación RFC 3261 del Grupo de Trabajo de Ingeniería de Internet (IETF), proporciona una normativa emergente para establecer sesiones multimedia sobre Internet. Sus capacidades básicas son la modificación del establecimiento y la supresión de cualquier sesión de comunicaciones, de manera que el mismo es un protocolo de señalización. El SIP proporciona también movilidad personal, lo cual significa que se puede acceder a un cliente a través de una única dirección con independencia de su punto actual de conexión a la red.

Para soportar servicios multimedia, una movilidad sin interrupciones y una conferencia multiusuario eficaz, es necesario mejorar la capa IP. El IP Móvil permite que los terminales se desplacen libremente entre diferentes redes móviles.

El SIP se usa para establecer, modificar y finalizar sesiones. Proporciona movilidad personal al permitir que un usuario se registre dinámicamente en la red con su dirección de comunicación, es decir, el URI (Indicador Uniforme de Recursos) SIP. Normalmente una sesión es una serie de flujos continuos a intercambiar del Protocolo de Transporte en Tiempo Real (RTP). Habitualmente, una sesión es una combinación de flujos continuos de voz, audio y vídeo, aunque también puede contener aplicaciones compartidas. Una red SIP básica está compuesta por cuatro tipos de elementos, es decir, Agentes de Usuario (UA), Servidores *Proxy*, Servidores de Redireccionamiento y Servidores de Registro. Los Agentes de Usuario residen típicamente en puntos extremos tales como teléfonos IP, ordenadores personales o dispositivos móviles. Los mismos inician solicitudes y proporcionan respuestas. Habitualmente, los UA disponen también de una interfaz para la gestión de los medios y para el software de aplicación concreto que proporciona la interfaz de usuario. Los servidores *proxy* son intermediarios, los cuales reciben y reenvían solicitudes que les proporcionan, por ejemplo, servicios de encaminamiento u otros servicios. Los servidores de redireccionamiento simplemente responden a una solicitud pidiendo a su originador que la redireccionen hacia una dirección nueva. Los servidores de registro mantienen un seguimiento de los puntos concretos de contacto de los clientes mediante la aceptación de registros de los UA. Los servidores de registro y el procedimiento de registro SIP en general proporcionan movilidad del usuario ya que se puede acceder al cliente desde cualquier ubicación a través de una única dirección. En este sentido, se parecen a la funcionalidad de los Registros de Posiciones Base (HLR) en las redes del Sistema Global para Comunicaciones Móviles (GSM). Cada cliente es parte de un dominio y cada dominio hace uso de por lo menos un servidor de registro, el cual conoce la ubicación de sus clientes en el caso de que los mismos se hayan registrado.

El SIP usa un formato de dirección común con el Correo de Internet, es decir, "usuario@dominio". La parte del dominio se usa para hallar el dominio correcto para el cliente y la parte de usuario se usa para diferenciar entre clientes individuales dentro de un dominio. El SIP incluye mensajes de solicitud y respuesta que comprenden campos de encabezamiento, por ejemplo, para definir a dónde se va a enviar a continuación la solicitud, la dirección del destinatario, la dirección del emisor, etcétera. Además, un mensaje SIP puede contener una parte de carga útil para transmitir información específica del abonado o del servicio.

Se observa que los flujos continuos RTP no siguen el mismo camino que el mensaje SIP, sino que fluyen directamente entre los dispositivos pertinentes. De este modo es posible enviar las solicitudes SIP subsiguientes directamente entre los UA. En un IMS, los mensajes SIP subsiguientes siguen el camino registrado en el encabezamiento *Record-Route* de la solicitud inicial, mientras que los nodos de la red interrogadores pueden retirarse y en el camino pueden quedarse otros elementos de la red. Por otro lado, los servidores *proxy* que se encuentran en medio pueden solicitar el quedarse en el camino de señalización mientras dure la llamada. Esta opción podría resultar útil en el caso de que el *proxy* ofrezca ciertos servicios para la llamada.

En la actualidad, el Proyecto de Asociación de Tercera Generación (3GPP) está especificando el IMS, por ejemplo, en su especificación TS 23.228, como un subsistema independiente del acceso el cual se puede usar en conexión con diferentes redes. El IMS usa el SIP para el inicio de la sesión. Básicamente, el IMS es simplemente un caso concreto de una red SIP. El mismo dispone de una serie de *proxies* y de un registrador. El UA está situado en el dispositivo terminal o equipo de usuario (UE). Cuando dos dispositivos establecen una sesión, los mismos hablan entre sí a través

de elementos de la Función de Control del Estado de la Llamada o la Función de Control de la Sesión de la Llamada (CSCF), mientras que los flujos de los medios RTP no pasan a través de las CSCF sino que van directamente entre los dispositivos. Un Servidor de Aplicaciones (AS) es un elemento SIP que gestiona servicios, tales como el control avanzado de llamadas, la presencia o la mensajería instantánea. El AS puede finalizar sesiones/transacciones. El AS también puede iniciar sesiones/transacciones, por ejemplo, en nombre de un usuario o un servicio.

No obstante, puede haber situaciones en las que el AS no sepa si debería comenzar a dar origen a o a finalizar servicios cuando recibe un mensaje de solicitud entrante, por ejemplo, un mensaje INVITACIÓN SIP, o una CSCF de servicio (S-CSCF) no sabe si el mensaje de solicitud entrante da inicio a una sesión/transacción de origen o de finalización. Por otra parte, puede que sea necesaria otra información para el equilibrado de la carga dentro de la red. Además, con fines relacionados con la compartición de la carga en un servidor de procesado de conexiones (CPS), especialmente en la S-CSCF y en una CSCF interrogadora (I-CSCF), es importante proporcionar un algoritmo rápido y sencillo para descubrir si una solicitud SIP recibida es la primera de una sesión SIP ó a qué sesión SIP pertenece una solicitud o respuesta recibida. En la actualidad, el SIP no proporciona unos medios eficaces del tipo mencionado. Para identificar un diálogo SIP, es decir, un tramo de llamada, identificado por una combinación de identificación, origen y destino de la llamada, un elemento de la red ó UE debe comparar los campos de encabezamiento respectivos de cada mensaje SIP y a continuación debe determinar si el tramo de la llamada ya existe. Esta situación implica comparaciones farragosas entre cadenas y consultas a bases de datos. Un elemento de red que mantiene un número elevado de tramos de llamada paralelos necesita una gran cantidad de recursos. Adicionalmente, en caso de un fallo en un elemento de la red, es necesaria información sobre las sesiones existentes.

Sumario de la invención

Por esta razón, uno de los objetivos de la presente invención es proporcionar un esquema eficaz de control de la carga para redes de datos por paquetes.

Este objetivo se alcanza a través de un método de control de la carga de procesado en una red de datos por paquetes, comprendiendo dicho método las etapas siguientes:

- fijar una información de control de carga en un campo predeterminado de un mensaje;

- encaminar dicho mensaje a través de esa red de datos por paquetes;

- comprobar dicha información de control de carga sobre la vía de encaminamiento de dicho mensaje y/o sobre la vía de encaminamiento de un mensaje de respuesta a dicho mensaje; y

- seleccionar un recurso de procesado de dicha red de datos por paquetes en respuesta al resultado de dicha etapa de comprobación.

Además, el objetivo anterior se alcanza por medio de un dispositivo de red para controlar la carga de procesado en una red de datos por paquetes, comprendiendo dicho dispositivo:

- unos medios de comprobación para comprobar una información de control de carga proporcionada en un campo predeterminado de un mensaje o mensaje de respuesta; y

- unos medios de selección para seleccionar un recurso de procesado para dicho mensaje o mensaje de respuesta en respuesta a dichos medios de comprobación.

Adicionalmente, el objetivo anterior se alcanza por medio de un dispositivo para transmitir un mensaje hacia una red de datos por paquetes, estando dispuesto dicho dispositivo para fijar en un campo predeterminado de dicho mensaje una información de control de carga para seleccionar recursos de procesado de dicha red de datos por paquetes.

Por otra parte, el objetivo anterior se alcanza a través de un método de distribución de información de control de carga en una red por conmutación de paquetes, que comprende las etapas siguientes:

- crear una primera información de control de carga para seleccionar recursos de procesado de dicha red de datos por paquetes en un primer elemento de red;

- fijar dicha primera información de control de carga en un campo predeterminado de un mensaje;

- encaminar dicho mensaje hacia un segundo elemento de red;

- almacenar dicha primera información de control de carga en dicho segundo elemento de red;

- crear una segunda información de control de carga para seleccionar recursos de procesado de dicha red de datos por paquetes en dicho segundo elemento de red;

- fijar dicha segunda información de control de carga en un campo predeterminado de un segundo mensaje;

- encaminar dicho segundo mensaje hacia dicho primer elemento de red; y

- almacenar dicha segunda información de control de carga en dicho primer elemento de red.

Adicionalmente, el objetivo anterior se alcanza por medio de un sistema para controlar la carga de procesado en una red de datos por paquetes, comprendiendo dicho sistema:

- un primer elemento de red para fijar una información de control de carga en un campo predeterminado de un mensaje a encaminar en dicha red de datos por paquetes; y

- un segundo elemento de red para comprobar dicha información de control de carga sobre la vía de encaminamiento de dicho mensaje; y para seleccionar un recurso de procesado de dicha red de datos por paquetes en respuesta al resultado de la comprobación.

Finalmente, el objetivo anterior se alcanza por medio de un sistema para distribuir información de control de carga en una red por conmutación de paquetes, comprendiendo dicho sistema:

- un primer elemento de red para crear una primera información de control de carga para seleccionar recursos de procesado de dicha red de datos por paquetes y para fijar dicha primera información de control de carga en un campo predeterminado de un mensaje; y

- un segundo elemento de red para recibir dicho mensaje, para almacenar dicha primera información de control de carga, para crear una segunda información de control de carga con vistas a seleccionar recursos de procesado de dicha red de datos por paquetes, para fijar dicha segunda información de control de carga en un campo predeterminado de un segundo mensaje, y para encaminar dicha segunda información de control de carga hacia dicho primer elemento de red;

en el que dicho primer elemento de red está adaptado para almacenar dicha segunda información de control de carga.

Por consiguiente, la información de compartición de carga o de equilibrado de carga se puede encaminar en mensajes hacia los nodos o servidores respectivos de la red para reducir de este modo la cantidad de recursos necesarios para la funcionalidad de control de carga. Por otra parte, en caso de fallos de elementos de la red se puede proporcionar información sobre sesiones existentes.

El campo predeterminado puede ser un parámetro *branch* del campo *via* de un mensaje SIP. La información de equilibrado de la carga se puede copiar desde otro campo predeterminado hacia dicho campo predeterminado.

El campo predeterminado puede ser un subcampo de una parte de usuario de un encabezamiento de dirección, por ejemplo, un URI del encabezamiento *Route* SIP. De este modo, en la parte del usuario se puede transportar información adicional. En particular, en uno o más subcampos se puede transportar información confidencial de la empresa, por ejemplo, información cifrada y/o tokenizada y/o codificada. Además, el encaminamiento dentro de un elemento de red, por ejemplo, la selección de un modelo de estados de llamadas correcto (por ejemplo, para dar origen a o finalizar un caso de sesión/transacción) se puede llevar a cabo usando el subcampo o subcampos de la parte de usuario. La información de control de carga y/u otras informaciones de control pueden ser una información específica del abonado y/o del servicio y/o del servidor transportada en uno o más subcampos, por ejemplo, desde una S-CSCF a un AS. Alternativamente, en el subcampo se puede transportar una dirección IP, la cual puede ser una dirección del anfitrión en la parte del dominio.

De este modo, en la parte del usuario se puede proporcionar una pluralidad de subcampos para transportar tipos diferentes de dicha información de control de carga y/o las otras informaciones de control. En particular, la parte del usuario se puede analizar sintácticamente y se puede dividir entre los subcampos. Alternativamente, por lo menos una de las características de entre estructura, orden y uso de los subcampos se puede predeterminar, por ejemplo, basándose en un esquema normalizado. Los subcampos se pueden separar por medio de una cadena de bits, un carácter, una cadena de caracteres, u otro separador predeterminados.

La etapa de selección se puede usar para el equilibrado de la carga. Para distribuir el mensaje hacia un nodo procesador predeterminado se puede usar una dirección virtual. La dirección virtual puede ser compartida por una pluralidad de nodos procesadores. Estos nodos procesadores pueden disponer de una funcionalidad de control del estado de la llamada de una red celular basada en IP. De este modo, se proporciona un mecanismo para garantizar un

equilibrado uniforme de la carga, y se puede vincular un abonado como nodo procesador durante todo el periodo de registro. Mediante el uso de una dirección virtual, una agrupación por sí misma puede realizar el equilibrado de la carga para nodos de la agrupación.

Adicionalmente, la información de control de carga puede comprender un primer número de puerto que indique un primer puerto para recibir un mensaje de solicitud. Además, la información de control de carga puede comprender un segundo número de puerto que indique un segundo puerto para recibir un mensaje de respuesta. De este modo, se pueden recibir solicitudes y respuestas en el puerto indicado en el que se proporciona una información de equilibrado de carga.

Según otro de los aspectos, la información de control de carga puede comprender una primera información y una segunda información opcional. La primera y la segunda información opcional se pueden fijar en un campo de un encabezamiento seleccionado de entre un campo de encabezamiento *Route*, un campo de encabezamiento *Via*, o un campo de encabezamiento *Contact* de un mensaje SIP. La primera información puede indicar si ya existe una sesión del mensaje. A continuación, la segunda información opcional puede indicar una identificación de la sesión existente. La primera y la segunda informaciones pueden ser informaciones ocultas no significativas para otras redes.

Por consiguiente se pueden proporcionar dos alternativas. En la primera alternativa, únicamente se detecta si el mensaje es el primero en un tramo de una llamada. De este modo, se puede proporcionar un reconocimiento sencillo y rápido del primer mensaje en una sesión. No es necesario ningún cambio en otros elementos o terminales de la red. El esquema se puede proporcionar incluso basándose en un diseño no normalizado. En la segunda alternativa, se detecta una identificación de sesión adicional basándose en la segunda información. De este modo, además de las ventajas anteriores de la primera alternativa, se puede proporcionar un reconocimiento sencillo y rápido de la sesión en cuestión.

En particular, la primera y/o la segunda informaciones se pueden fijar como parte de la parte de usuario de una dirección (por ejemplo, URI SIP) de un campo del encabezamiento, como parte del nombre de anfitrión de un campo del encabezamiento, como parte del nombre del dominio de un campo del encabezamiento, como parámetro del campo del encabezamiento, como número de puerto del campo del encabezamiento, en el que el número del puerto se puede usar para diferenciar un primer mensaje con respecto a mensajes subsiguientes, o como un campo de encabezamiento de extensión para el mensaje. Alternativamente, la primera y/o la segunda informaciones se pueden fijar en una parte de carga útil del mensaje.

A continuación, la segunda información se puede extraer en respuesta a una detección de la primera información, y se puede usar en la etapa de selección.

El dispositivo de red para controlar la carga de procesado puede comprender una funcionalidad de control del estado de la llamada o de la sesión de la llamada de una red celular basada en IP. Los medios de selección pueden estar dispuestos para seleccionar un nodo procesador predeterminado hacia el cual se distribuye dicho mensaje. De este modo, además de la dirección virtual, la información de control de carga especifica el nodo procesador.

Los medios de selección pueden estar dispuestos para iniciar la creación de una sesión nueva.

El dispositivo para transmitir el mensaje puede comprender también una funcionalidad de control del estado de la llamada o funcionalidad del control de la sesión de la llamada de la red celular basada en IP. Esta funcionalidad de control de la sesión puede ser una funcionalidad de control de la sesión de la llamada de servicio, una funcionalidad de control de la sesión de la llamada interrogadora o una funcionalidad de control de sesión de la llamada *proxy*. El dispositivo puede estar dispuesto para fijar la información de control de carga en la parte de usuario de la dirección del encabezamiento del mensaje, o, alternativamente, en un nombre de anfitrión, un nombre de dominio, un parámetro del encabezamiento, un número de puerto, o un campo del encabezamiento de extensión correspondiente a una parte de encabezamiento o en una parte de carga útil del mensaje.

En las reivindicaciones subordinadas se definen otras evoluciones ventajosas de la presente invención.

Breve descripción de los dibujos

A continuación se describirá la presente invención basándose en formas de realización preferidas y haciendo referencia a los dibujos adjuntos, en los cuales:

la Fig. 1 muestra una arquitectura de red IMS en la cual se puede implementar la presente invención;

la Fig. 2 muestra una estructura de un URI SIP según la primera forma de realización preferida;

la Fig. 3 muestra un diagrama de señalización y procesado de un primer ejemplo de señalización según la primera forma de realización preferida;

la Fig. 4 muestra un diagrama de procesado y señalización que indica un segundo ejemplo de señalización según la primera forma de realización preferida;

la Fig. 5 muestra un diagrama de señalización y procesado de acuerdo con una segunda forma de realización preferida;

la Fig. 6 muestra un diagrama de flujo de un primer ejemplo de un mecanismo de compartición de la carga de acuerdo con la segunda forma de realización preferida; y

la Fig. 7 muestra un diagrama de flujo de un segundo ejemplo de un mecanismo de compartición de la carga de acuerdo con la segunda forma de realización preferida.

Descripción de la forma de realización preferida

A continuación se describirán las formas de realización preferidas basándose en una arquitectura de red IMS según se muestra en la Fig. 1.

Debe indicarse que la Fig. 1 únicamente muestra aquellos componentes IMS necesarios para una descripción de la presente invención. Como ejemplo, en la Fig. 1 no se muestran la red de acceso de radiocomunicaciones y la red central. Según la Fig. 1, un dispositivo terminal ó UE 10, el cual puede ser un dispositivo terminal móvil o celular, se conecta a una P-CSCF 20 dispuesta en un dominio visitado 70 del UE 10 y que proporciona una conectividad IP básica y una gestión móvil por debajo de la primera. El UE 10 usa el SIP para comunicarse con la P-CSCF 20 la cual es similar a un servidor *proxy* SIP. En el presente caso, el cliente o abonado del UE 10 se está desplazando de forma itinerante en el dominio visitado 70 en el que está ubicada la P-CSCF 20. La función de la P-CSCF 20 es proporcionar llamadas de emergencia y otros servicios de este tipo que requieren un conocimiento específico del dominio visitado 70. En lugar de una red de acceso de radiocomunicaciones también se pueden usar redes de acceso alternativas. En lugar del dispositivo terminal móvil celular, también se pueden usar otros tipos de terminales, especialmente en redes de acceso alternativas.

Además, en el dominio de origen 80 del abonado o cliente hay siempre ubicada una S-CSCF 40 y la misma adopta la función de los servidores de registro y *proxy* SIP, de manera que el UE 10 se puede registrar en la S-CSCF 40 usando el SIP a través de la P-CSCF 20. Además, se proporciona una I-CSCF 30 como servidor *proxy* SIP adicional responsable principalmente de hallar la S-CSCF correcta para un abonado o cliente determinado. Las S-CSCF se pueden asignar dinámicamente por cada registro con vistas a conseguir un equilibrado eficaz de la carga y una residencia de los errores. Se proporciona un Servidor de Aplicaciones (AS) 60 como elemento SIP que trata los servicios proporcionados al UE 10. Se pueden proporcionar AS independientes con fines diferentes. Finalmente, un Servidor de Abonado de Origen (HSS) 50 está dispuesto para la gestión y autenticación de perfiles.

A continuación se describirá una primera forma de realización preferida de la presente invención basándose en las Figs. 2 a 6.

En la primera forma de realización preferida, para el control de la carga, por ejemplo, el control de las sesiones y el equilibrado de la carga, se usa un contenido de una parte de usuario del URI SIP. En particular, la parte de usuario del URI (Identificador Uniforme de Recursos) SIP se puede dividir en subcampos los cuales se pueden utilizar con finalidades, por ejemplo, de control y/o encaminamiento. En el SIP, el Encabezamiento *Route* contiene normalmente identificadores URI SIP los cuales tienen únicamente una parte de dominio, de tal manera que la parte de usuario queda libre para ser usada con otros fines.

La Fig. 2 muestra un diagrama esquemático que indica una estructura del FQDN ó URI SIP 100 según la primera forma de realización preferida. El URI SIP 100 comprende una parte de usuario 120 y una parte de dominio 140 separadas por un símbolo "@", de forma similar a una dirección de correo electrónico. Los objetos direccionados por el SIP son usuarios en anfitriones, identificados por el URI SIP 100. La parte de usuario 120 se usa para transportar un nombre de usuario o un número de teléfono, mientras que la parte de anfitrión o dominio 140 transporta bien un nombre dominio o bien una dirección de red numérica.

Debido al hecho de que la parte de usuario no se usa en el encabezamiento *Route* ni en el encabezamiento *Via*, la misma se puede dividir entre los subcampos 121, 122, ... 12n, los cuales se pueden separar mediante un separador adecuado 130, por ejemplo, una cadena de bits, un carácter o una cadena de caracteres, en la que los caracteres pueden ser caracteres imprimibles y/o no imprimibles o cadenas de bits. El orden y uso de los subcampos 121 a 12n se puede predeterminar o normalizar en el caso de que no se considere como una información específica de la implementación.

En relación con la disposición en la estructura de los subcampos 121 a 12n en la parte de usuario 120, se pueden usar tres opciones.

Según la primera opción, la parte de usuario 120 se puede disponer como un único campo, el cual contiene los subcampos 121 a 12n. A continuación, este campo único se analiza sintácticamente y, cuando sea necesario, se divide entre los subcampos 121 a 12n. Esta situación proporciona la ventaja de que no es necesaria ninguna normalización si el campo se crea y se utiliza dentro de la misma red.

De acuerdo con la segunda opción, la parte de usuario 120 puede constar estructuralmente de los subcampos 121 a 12n, mientras que la sintaxis y posiblemente también la semántica de los subcampos 121 a 12n están predefinidas o normalizadas. En este caso, los subcampos 121 a 12n se pueden crear y utilizar incluso en redes diferentes.

Según la tercera opción, se puede usar una combinación de la primera y la segunda opciones.

El siguiente es un ejemplo del URI SIP 100 en el que se usa un segundo subcampo para señalizar el caso de sesión/transacción y se usa un primer subcampo para señalizar una información específica de la implementación. El separador 130 se forma con el corrector "_".

57BC442C_finalización@s-cscf2.ims.sosnera.fi

Por consiguiente, "finalización" se señaliza como el caso de la sesión/transacción y "57BC442C" se señaliza como la información específica de la implementación.

A continuación se describen un primer y un segundo ejemplos de un mecanismo de control de carga según la primera forma de realización preferida haciendo referencia a las Figs. 3 y 4.

El mecanismo de control de carga se proporciona para garantizar un equilibrado uniforme de la carga en el caso de que un elemento o parte de la red se implemente mediante una serie de nodos procesadores. En la arquitectura de la red IMS según la Fig. 1, el UE 10 dispone de la P-CSCF 20 como punto de contacto con la red. Entre el UE 10 y la P-CSCF 20, se usa una función de seguridad IP IPSec para la protección de la integridad y la confidencialidad. Además, se puede usar una función de compresión para comprimir la información de señalización en la parte de prefijo o usuario 120 del FQDN ó URI SIP 100 del UE 10. Para lograr una capacidad elevada y unos tiempos de respuesta rápidos, los datos IPSec y los datos de compresión del abonado específico del UE 10 se deben almacenar en una memoria, por ejemplo, una memoria volátil o una memoria de acceso aleatorio (RAM). Como consecuencia, un abonado debería quedar vinculado al nodo procesador en el cual se ha registrado. Mediante el uso de la dirección virtual, únicamente la propia agrupación de nodos o servidores puede realizar el equilibrado de la carga para los nodos de la agrupación.

La Fig. 3 muestra un diagrama de señalización y procesado de un mecanismo de control de carga para distribuir una información de equilibrado de carga (LBI) al producirse el registro de un usuario. En este caso, el razonamiento para el equilibrado de la carga es que, por ejemplo, la compresión se realiza en nodos distribuidos. Por esta razón, en la práctica, en la interfaz entre el UE 10 y la P-CSCF 20 no se puede realizar un equilibrado de la carga basándose en la información del nivel SIP ya que la misma está comprimida. En esta interfaz, la clave razonable para el equilibrado de la carga es la dirección IP del UE 10. Cuando se recibe un intento o solicitud de finalización, el cual va dirigido al UE 10, es esencial que el intento de finalización se reciba en el mismo nodo de procesado hacia el cual se distribuyen los mensajes del UE 10. De este modo, se pueden evitar saltos innecesarios en la red basada en IP.

Cuando el UE 10 transmite en la etapa 1 un mensaje Registro SIP, la P-CSCF 20 crea e inserta en la etapa 2 una primera información de equilibrado de carga LBI(P-CSCF-1) en el URL-SIP(P-CSCF) del campo *Path* del encabezamiento de ese mensaje Registro. La primera información de equilibrado de carga LBI(P-CSCF-1) del campo *Path* se recibirá posteriormente cuando se reciba una solicitud inicial desde la S-CSCF 40. La P-CSCF 20 también crea e inserta una segunda información de equilibrado de carga LBI(P-CSCF-2) en el parámetro *branch* del campo *Via* en dicho mensaje Registro. La segunda información de equilibrado de carga LBI(P-CSCF-2) en el parámetro *branch* del campo *Via* se recibirá junto con una respuesta a dicho mensaje Registro. La primera y la segunda informaciones de equilibrado de carga LBI(P-CSCF-1) y LBI(P-CSCF-2) pueden ser idénticas o diferentes. El mensaje de registro se encamina en la etapa 3 y 4 a través de la I-CSCF 30 hacia la S-CSCF 40. Cuando la S-CSCF 40 recibe el mensaje Registro desde la P-CSCF 20, realizan un equilibrado de la carga en la etapa 5 basándose en, por ejemplo, la ID de la Llamada. En la etapa 6, la S-CSCF 40 almacena a continuación en una base de datos de abonado el URL-SIP(P-CSCF) del campo *Path*, el cual contiene la primera información de equilibrado de carga LBI(P-CSCF-1) de la P-CSCF 20. En la etapa 7, la S-CSCF 40 crea una información de equilibrado de carga propia LBI(S-CSCF-1) y la inserta en el URL-SIP(S-CSCF) del campo *Service-Route* del mensaje de respuesta SIP 200OK enviado en las etapas 8 y 9 a través de la I-CSCF 30 hacia la P-CSCF 20. Esta información de equilibrado de carga LBI(S-CSCF-1) se recibirá en el futuro cuando se reciba una solicitud inicial desde la P-CSCF 20. Adicionalmente, el parámetro *branch* del campo *Via* contiene el URL-SIP(P-CSCF) de la P-CSCF 20 que se ha copiado a partir del mensaje inicial Registro recibido después de la etapa 4. Cuando la P-CSCF 20 recibe este mensaje de respuesta 200OK, en la etapa 10 se puede realizar el equilibrado de carga basándose en la segunda información de equilibrado de carga LBI(P-CSCF-2) obtenida a partir del parámetro *branch* del campo *Via*. En la etapa 11, la P-CSCF 20 almacena en una base de datos el URL-SIP(S-CSCF) que contiene la información de equilibrado de carga LBI(S-CSCF-1) de la S-CSCF 40 obtenida a partir del campo *Service Route* del mensaje de respuesta 200OK. Finalmente, en la etapa 12, se reenvía hacia el UE 10 el mensaje de respuesta 200OK que indica un registro satisfactorio.

Por consiguiente, después del procedimiento anterior, la P-CSCF 20 dispone del URL-SIP(S-CSCF) en sus datos de abonado, el cual apunta a la S-CSCF 40 y contiene la información de equilibrado de carga correspondiente LBI(S-CSCF-1). De forma similar, la S-CSCF 40 dispone del URL-SIP(P-CSCF) en sus datos de abonado, el cual apunta a la P-CSCF 20 y contiene la información de equilibrado de carga correspondiente LBI(P-CSCF-1). De este modo, la información de equilibrado de carga puede ser usada posteriormente por los equilibradores de carga respectivos de la P-CSCF 20 y la S-CSCF 40. Por ejemplo, cuando se produce un intento de finalización, a continuación la S-CSCF

40 va a buscar esta información de equilibrado de carga a la base de datos de abonado y la inserta en la solicitud correspondientes.

La Fig. 4 muestra un diagrama de procesado y señalización de un mecanismo control de carga para usar la información de equilibrado de carga (LBI) cuando se envía una solicitud de inicio a la red. Cuando en la etapa 1 el UE 10 envía un mensaje Invitación SIP a la P-CSCF 20, se realiza un equilibrado de carga basándose en la dirección IP del UE 10. En la etapa 2, la P-CSCF 20 lee de la base de datos de abonado el URL-SIP(S-CSCF) almacenado anteriormente que se usará para encaminar el mensaje Invitación hacia la S-CSCF40 en la etapa 3. Adicionalmente, el URL-SIP(S-CSCF) se inserta en el campo *Route* superior, y el URL-SIP(P-CSCF) se inserta en el campo *Record-Route*. Por otra parte, la primera información de equilibrado de carga LBI(P-CSCF-1) se inserta en el parámetro *branch* del campo *Via*. Cuando se recibe el mensaje Invitación en la S-CSCF 40, esta última obtiene, a partir del campo *Route* superior, el URL-SIP(S-CSCF) que contiene su información de equilibrado de carga fijada anteriormente LBI(S-CSCF-1). Basándose en esta información de equilibrado de carga LBI(S-CSCF-1), en la etapa 4 se realiza un equilibrado de la carga para hallar un ordenador correcto. Cuando la S-CSCF 40 envía el mensaje Invitación en la etapa 5, inserta el URL-SIP(S-CSCF) en el campo *Record-Route* e inserta su información de equilibrado de carga LBI(S-CSCF-1) en el parámetro *branch* del campo *Via*. En la etapa 6, el servidor de aplicaciones 60 responde con un mensaje de respuesta 200OK que comprende la información de equilibrado de carga LBI(P-CSCF-1) y LBI(S-CSCF-1) de la P-CSCF 20 y la S-CSCF 40 en el parámetro *branch* del campo *Via*. Cuando la S-CSCF 40 recibe el mensaje de respuesta 200OK, la misma obtiene su información de equilibrado de carga LBI(S-CSCF-1) a partir del parámetro *branch* del campo *Via* y la usa para el equilibrado de la carga en la etapa 7. De forma similar, cuando la P-CSCF 20 recibe subsiguientemente el mensaje de respuesta 200OK reenviado por la S-CSCF 40 en la etapa 8, la misma obtiene su primera información de equilibrado de carga LBI(P-CSCF-1) a partir del parámetro *branch* del campo *Via* y la usa para el equilibrado de carga en la etapa 9. En la etapa 10, el mensaje 200OK se reenvía hacia el UE 10 para acusar el recibo del mensaje Invitación anterior.

Cuando el servidor de aplicaciones 60 envía en la etapa 11 una solicitud SIP subsiguiente, por ejemplo, un mensaje Invitación, dentro de un diálogo, el mismo usa una lista *Route* que ha creado anteriormente basándose en las entradas *Record-Route* de la solicitud inicial, es decir, el mensaje Invitación recibido después de la etapa 5. La entrada *Route* superior es el URL-SIP(S-CSCF) que incluye en su interior la información de equilibrado de carga correspondiente LBI(S-CSCF-1). La segunda entrada *Route* es el URL-SIP(P-CSCF) que incluye en su interior la información de equilibrado de carga correspondiente LBI(P-CSCF-1). Cuando la S-CSCF 40 recibe el mensaje Invitación subsiguiente, la misma obtiene a partir de la entrada *Route* superior su información de equilibrado de carga LBI(S-CSCF-1) que se encuentra dentro del URL-SIP(S-CSCF). En la etapa 12, la S-CSCF 40 realiza un equilibrado de la carga basándose en esta información de equilibrado de carga LBI(S-CSCF-1) y elimina la entrada *Route* que apunta le apunta. A continuación, la entrada *Route* superior apunta a la P-CSCF 20. En la etapa 13, el mensaje Invitación subsiguiente se reenvía hacia la P-CSCF 20. Cuando la P-CSCF 20 recibe el mensaje Invitación subsiguiente, obtiene a partir de la entrada *Route* superior su información de equilibrado de carga LBI(P-CSCF-1) que se proporciona dentro del URL-SIP(P-CSCF). A continuación, realiza un equilibrado de la carga basándose en esta información de equilibrado de carga LBI (P-CSCF-1) en la etapa 14, y elimina la entrada *Route* que le apunta. Finalmente, en la etapa 15, el mensaje Invitación se reenvía hacia el UE 10.

En general, en la fase de registro, la información del camino y de equilibrado de carga se registra y almacena para ser usada posteriormente para solicitudes. La solicitud posterior debería contener esta información de equilibrado de carga, y a continuación el equilibrado de la carga se realiza basándose en dicha información de equilibrado de carga. Por consiguiente, cualquier información de equilibrado de carga insertada durante la fase de registro está destinada a futuras solicitudes.

En todos los casos, se puede usar el parámetro *via-branch* del campo *Via* del encabezamiento para transportar información similar usada por la función de equilibrado de carga para distribuir respuestas hacia el nodo procesador correcto.

Además, se pueden usar diferentes números de puerto para identificar en dónde se puede hallar la información de equilibrado de carga. En particular, durante el "registro del camino", el puerto de solicitud se fija en la parte de dominio 140 del URI SIP 120. De este modo, a continuación las solicitudes se reciben en dicho puerto de solicitud y se sabe dónde leer la información de equilibrado de carga. Se puede fijar un "puerto" similar para las solicitudes salientes, de tal manera que las respuestas se reciban en ese puerto.

En el caso de una función de equilibrado de carga para un tráfico SIP de ingreso entrante que vaya destinado al elemento de red en cuestión, se comprueba si la dirección IP de destino es o no una dirección IP virtual. En caso negativo, no es necesario el equilibrado de la carga, a continuación se puede aplicar, por ejemplo, un encaminamiento L3 normal para el paquete. Si la dirección IP de destino es una dirección IP virtual, en ese caso es necesario un equilibrado de la carga. Existen dos opciones, es decir, la dirección IP virtual puede ser bien una dirección P-CSCF ó bien una dirección S-CSCF ó I-CSCF. Para detectar el tipo y la ubicación de información de equilibrado de carga se usa una información correspondiente del puerto de destino. A continuación, se realiza un equilibrado de la carga basándose en la información de equilibrado de carga y la salida resultante se corresponde con el nodo de procesado correcto hacia el que se deberían reenviar los paquetes. La información de equilibrado de carga puede ser una id de llamada, una dirección IP-UE, o una información de equilibrado de carga generada anteriormente.

En el caso de un tráfico de egreso o saliente que se origine en el elemento de red en cuestión, se comprueba la dirección IP de origen para ver si es una de las direcciones IP virtuales (P-CSCF, S-CSCF ó I-CSCF) del CPS. En caso negativo, a continuación se produce un encaminamiento normal. En caso afirmativo, se comprueba si es una dirección de Bucle. Si es así, se determina el protocolo de transporte y subsiguientemente se comprueba el puerto de destino para determinar un puerto de solicitud o puerto dedicado. Sobre la base del resultado de la comprobación, se selecciona un procedimiento para obtener la información de equilibrado de carga y reenviar el paquete IP. En caso de que sea una Dirección No de Bucle, se comprueba nuevamente la dirección IP de origen para determinar si la misma es una dirección S-CSCF/I-CSCF ó una dirección P-CSCF. Si la misma es una dirección S-CSCF/I-CSCF, se determina el protocolo de transporte, es decir, el Protocolo de Control de Transmisión (TCP) o el Protocolo de Datagrama de Usuario (UDP). Si se indica el TCP, se vuelve a ensamblar el mensaje SIP después de almacenarlo temporalmente y a continuación el mismo se reenvía. Si se indica el UDP, el paquete IP se puede reenviar directamente. Si la dirección es una dirección P-CSCF, se determina el puerto de origen. Si se indica un puerto de Cliente o puerto de Solicitud, se determina el protocolo de transporte y se inicia nuevamente el procesado anterior. En el caso de que se indique un puerto del cliente/servidor no seguro/seguro UE, el paquete IP es reenviado directamente por un procedimiento L3 (Capa de Protocolo 3).

A continuación se describe la segunda forma de realización preferida de la presente invención haciendo referencia a las Figs. 5 a 7. La segunda forma de realización preferida trata sobre un mecanismo de compartición de carga para descubrir de una forma eficaz qué tráfico SIP pertenece a qué sesión, y si una solicitud, por ejemplo, una solicitud INVITACIÓN SIP, es una solicitud inicial o una repetición de una solicitud.

La Fig. 5 muestra un diagrama de procesado y señalización que indica un primer ejemplo del mecanismo de compartición de carga de acuerdo con la segunda forma de realización preferida. El mecanismo del primer ejemplo está adaptado para detectar si una solicitud SIP, por ejemplo, INVITACIÓN SIP, es la primera en un tramo de una llamada. Esto se logra proporcionando una información oculta en el campo de encabezamiento *Record-Route* de la solicitud SIP.

Siempre que una CSCF con estados de la sesión, por ejemplo, la S-CSCF 40 de la Fig. 1, reciba una solicitud SIP e inserte un campo de encabezamiento *Record-Route* (etapa 1), insertará una indicación oculta en el campo de encabezamiento *Record-Route* (etapa 2), y reenviará la solicitud SIP con la indicación oculta hacia la dirección de destino. En el presente caso, "oculta" significa que la indicación no tiene ningún significado para otras redes, por ejemplo, redes que se encuentran fuera de la red en la que se fija la indicación. No obstante, si fuera necesario, la indicación añadida también puede ser una información normalizada legible por otras redes.

A continuación, siempre que llegue una INVITACIÓN, una CSCF con estados de la sesión comprueba si el campo de encabezamiento *Route* superior o el URI de solicitud (en el caso de que no se disponga de encabezamiento *Route*) contiene dicha información oculta. El campo de encabezamiento *Route* se construye a partir del campo de encabezamiento *Record-Route*. Si la información o indicación oculta está presente, la sesión ya existe. En caso negativo, debe crearse internamente una sesión nueva en la CSCF con estados de sesión en cuestión.

Como las respuestas SIP (por ejemplo, 200 OK) en un caso normal pertenecen a una sesión existente, no es necesario diferenciar las mismas.

La indicación puede ser parte del nombre de anfitrión. Como ejemplo, se supone que la dirección de encaminamiento por defecto para este elemento sería <scscf17.operador.net> por ejemplo <B@proveedor.net; maddr=scscf17.operador.net>, y en ese caso el *Record-Route* podría tener este aspecto:

RecordRoute:<B@proveedor.net; maddr=exist.scscf17.operador.net>

o

Record-Route:<B@exist.proveedor.net>

o

Record-Route:<B@exist.scscf17.operador.net>

En este caso la indicación oculta sería "exist." como parte del nombre de anfitrión. La parte de usuario 120 en estos ejemplos puede estar vacía. Por ejemplo, en lugar de *<B@exist.scscf17.operador.net>* puede usarse la siguiente opción: *<exist.scscf17.operador.net>*. El campo de encabezamiento *Route* se construye a partir del campo de encabezamiento *Record-Route*. Por ejemplo:

Record-Route:<B@exist.scscf17.operador.net>

resulta en

Route:<B@exist.scscf17.operador.net>

Como alternativa, la S-CSCF 40 puede añadir un "rr-param" al campo de encabezamiento *Record-Route* según se define en la RFC3261:

*Record-Route = "RecordiRoute" HCOLON rec-route *(COMMA rec-route)*

*rec-route = name-addr *(SEMI rr-param)*

rr-param = generic-param

generic-param = token [EQUAL gen-value]

gen-value = token/host/quoted-string

token = 1(alphanum /"-"/"."/"!"/"%"/"*"*
/"_"/ "+"/"`"/"'"/"~")

*Route = "Route" HCOLON route-param *(COMMA route-param)*

*route-param = name-addr *(SEMI rr-param)*

Un ejemplo correspondiente puede tener el siguiente aspecto:

RecordRoute: <B@proveedor.net;maddr=scscf17.operador.net; existing>

o

Record-Route: <B@proveedor.net; existing>

o

Record-Route: <B@scscf17.operador.net; existing>

Nuevamente, la parte de usuario 120 puede estar vacía. El campo de encabezamiento *Route* se construye a partir del campo de encabezamiento *Record-Route*.

Si se recibe el rr-param "existing", se puede detectar fácilmente que la solicitud pertenece a una sesión existente.

Según una alternativa adicional, se pueden usar diferentes números de puerto para la primera solicitud y para las solicitudes subsiguientes. Por ejemplo, se supone que el encaminamiento por defecto para el elemento o nodo en cuestión sería <B@proveedor.net; maddr=scscf17.operador.net>. En este caso, la entrada *RecordRoute* podría tener este aspecto:

RecordRoute: <B@proveedor.net; maddr=scscf17.operador.net: 19373>

o

Record-Route: <B@proveedor.net: 19373>

o

Record-Route: <B@scscf17.operador.net: 19373>

Y nuevamente en este caso, la parte de usuario 120 puede estar vacía. El campo de encabezamiento *Route* se construye a partir del campo de encabezamiento *Record-Route*. Por ejemplo

Record-Route: <B@proveedor.net; maddr=scscf17.operador.net: 19373>

resulta en

Route: <B@proveedor.net; maddr=scscf17.operador.net: 19373>

Todas las solicitudes que llegan al puerto 19373 se reconocerían como pertenecientes a una sesión existente.

Según otra de las alternativas, para transportar la información, en el SIP se puede usar un campo de encabezamiento de extensión nuevo privativo o no normalizado. Un ejemplo de la entrada nueva del encabezamiento puede tener el siguiente aspecto:

CSCF-session: existing in scscf17.operador.net

No obstante, en este caso, el UA debería soportar esta característica, es decir, copiar este campo de encabezamiento nuevo desde las solicitudes SIP a las respuestas SIP y las solicitudes SIP subsiguientes.

Según todavía otra de las alternativas, para transportar la indicación oculta se podría usar la parte de carga útil de la solicitud SIP.

La Fig. 6 muestra un diagrama de flujo esquemático que indica el mecanismo de compartición de carga según el primer ejemplo. Cuando el elemento gestiona una solicitud inicial, en la solicitud se puede insertar el encabezamiento *Record-Route* antes de dar salida a la misma. A este encabezamiento *Record-Route* se le puede añadir una información oculta. Posteriormente, estos encabezamientos *Record-Route* se trasladan de vuelta dentro de la respuesta hacia el originador de la solicitud. Cuando el originador obtiene esta respuesta, recupera dichos encabezamientos *Record-Route* y los copia en la lista *Route*. Cuando el originador envía una solicitud subsiguiente, toma esta lista *Route* e inserta todas las entradas en la solicitud subsiguiente como encabezamiento *Route*. En este momento, se puede dar salida a la solicitud subsiguiente. Cuando el siguiente servidor recibe esta solicitud, el mismo puede hallar, a partir del encabezamiento *Route*, el mismo URI SIP que insertó anteriormente en la solicitud inicial. En la solicitud se inserta también un encabezamiento *Via*. En la respuesta a la solicitud se recibe el mismo encabezamiento *Via*, y la información oculta del encabezamiento *Via* se puede usar para hallar la instancia o elemento al cual debe trasladarse la respuesta.

De este modo, según la Fig. 6, si se recibe una solicitud SIP, se comprueba el campo de encabezamiento *Route*, o el campo de encabezamiento nuevo o la parte de carga útil, en relación con la indicación oculta (etapa S201). Si en la etapa S202 se detecta una indicación oculta, ya existe una sesión y no se requiere ninguna creación y la solicitud se puede asignar al tramo de llamada de la sesión existente (etapa S204). Por otro lado, si no se detecta ninguna indicación oculta, en la etapa S203 se crea una sesión nueva.

De acuerdo con el segundo ejemplo del mecanismo de compartición de carga, basándose en la indicación oculta se detecta un identificador de sesión interno (ISId). Esta alternativa incluye el mecanismo anterior del primer ejemplo, es decir, si no se puede descubrir el ISId, se puede suponer que la solicitud pertenece a un tramo de llamada nuevo.

En el segundo ejemplo, se proporciona una indicación oculta, por ejemplo, en el campo de encabezamiento *Record-Route* y en el campo de encabezamiento *Via* de la solicitud SIP.

De este modo, haciendo referencia a la Fig. 5, siempre que una CSCF con estados de la sesión, por ejemplo, la S-CSCF 40, inserte un campo de encabezamiento *Record-Route* o *Via*, la misma añadirá una indicación oculta, que contiene información sobre el identificador de sesión interno (ISId).

La Fig. 7 muestra un diagrama de flujo esquemático que indica el mecanismo mejorado de compartición de carga según el segundo ejemplo. Siempre que llega un mensaje, se comprueba si el mensaje se corresponde con una solicitud SIP (etapa S301). En caso afirmativo, la CSCF con estados de la sesión comprueba en la etapa S303 si el campo de encabezamiento *Route* superior contiene una indicación oculta. Si en la etapa S305 se determina que está presente la indicación oculta, la sesión existe y se puede extraer el ISId para proporcionar una función rápida de reconocimiento y asignación de la sesión (etapa S307). En caso negativo, en la etapa S306 debe crearse una sesión nueva.

Si en la etapa S301 no se detecta ninguna solicitud SIP, en la etapa S302 se comprueba si el mensaje se corresponde con una respuesta SIP. En caso afirmativo, la CSCF con estados de la sesión comprueba en la etapa S304 si el campo de encabezamiento *Via* superior contiene una indicación oculta. Si en la etapa S305 se determina que la indicación oculta está presente, la CSCF con estados de la sesión extrae el ISId del campo de encabezamiento *Via* superior de la respuesta SIP (etapa 307).

Por lo tanto, en las CSCF se puede proporcionar incluso una identificación rápida de una sesión existente.

Tal como en el primer ejemplo, la indicación oculta puede ser parte del nombre de anfitrión. Como ejemplo, se supone que el encaminamiento por defecto para este elemento sería <scscf17.operador.net> por ejemplo <B@proveedor.net; maddr=scscf17.operador.net>. En este caso, el campo de encabezamiento *Route* podría tener el siguiente aspecto. El campo de encabezamiento *Route* se construye a partir del campo de encabezamiento *Record-Route*.

Route: B@proveedor.net; maddr=ISId224497.scscf17.operador.net

o

Route: <B@ISId224497.proveedor.net>

o

Route: <B@ISId224497.scscf17.operador.net>.

En este caso, el ISId es “224497” como parte del nombre de anfitrión. La parte de usuario 120 puede estar vacía.

De forma similar, se podría usar el campo de encabezamiento *Via*, el cual en ese caso podría tener este aspecto:

Via: SIP/2.0/UDP ISId224497.scscf17.operador.net:5060

Todas las respuestas SIP que contienen “ISId224497” como parte del nombre de anfitrión pertenecen a la misma sesión existente.

De forma opcional, el ISId como parte del nombre de anfitrión también se podría cifrar/tokenizar para ocultarlo o con fines relacionados con la redundancia.

Como alternativa, la S-CSCF 40 puede añadir un “rr-param” al campo de encabezamiento *Record-Route* según se define en la RFC3261.

De forma similar, esta opción funciona para respuestas SIP, en las que el campo de encabezamiento *Via* se ampliaría mediante una “via-extension” según se define en la RFC3261:

```
Via      = (Via" / "v") HCOLON via-parm *(COMMA via-parm)

via-parm = sent-protocol LWS sent-by *(SEMI via-params)

via-params     = via-ttl/via-maddr

                 /via-received/via-branch

                 /via-extension

via-ttl   = "ttl" EQUAL ttl

via-maddr      = "maddr" EQUAL host

via-received   = "received" EQUAL (IPv4address / IPv6address)

via-branch     = "branch" EQUAL token

via-extension  = generic-param

sent-protocol  = protocol-name SLASH protocol-version

                 SLASH transport

protocol-name          = "SIP" / token

protocol-version =     token

transport      ,   =   "UDP" / "TCP" / "TLS" / "SCTP"/
other-transport

sent-by                = host [COLON port]

ttl                    = 1*3DIGIT; 0 to 255

generic-param = token [EQUAL gen-value]

gen-value      = token / host / quoted-string

token   = 1*(alphanum / "-" / "." / "!" / "%" / "*"
/ "_" / "+" / "`" / "'" / "~" )
```

En este caso, como ejemplo, el campo de encabezamiento *Route* podría tener el siguiente aspecto. El campo de encabezamiento *Route* se construye a partir del campo de encabezamiento *Record-Route*.

Route: <B@proveedor.net; maddr=scscf17.operador.net; ISId=224497>

o

Route: <B@proveedor.net; ISId=224497>.

o

Route: <B@scscf17.operador.net; ISId=224497>.

En este caso, el ISId es "224497" como parámetro del campo de encabezamiento *Route*.

Así, el campo de encabezamiento *Via* correspondiente podría tener este aspecto:

Via: SIP/2.0/UDP scscf17.operador.net:5060; ISId=224497.

En este caso, todas las respuestas SIP que contienen el parámetro "ISId=224497" pertenecen a la misma sesión existente.

Opcionalmente, el ISId como parte del nombre de anfitrión también se podría cifrar/tokenizar para ocultarlo o con fines relacionados con la redundancia.

Según una alternativa adicional, se pueden usar diferentes números de puerto para todas las sesiones existentes:

Como ejemplo, se supone que el encaminamiento por defecto para el elemento en cuestión sería <B@proveedor.net; maddr=scscf17.operador.net>, y en este caso el campo de encabezamiento *Route* podría tener el siguiente aspecto. El campo de encabezamiento *Route* se construye a partir del campo de encabezamiento *Record-Route*.

Route: <B@proveedor.net; maddr=scscf17.operador.net: 224497>

o

Route: <B@proveedor.net: 224497>

o

Route: <B@scscf17.operador.net: 224497>.

La parte de usuario puede estar vacía. En este caso, todas las solicitudes SIP que llegan, por ejemplo, al puerto 224497, pertenecen a la misma sesión existente.

De forma similar, esta opción funciona para el campo de encabezamiento *Via*, el cual podría tener este aspecto:

Via: SIP/2.0/UDP scsc17.operador.net: 224497

En este caso, todas las respuestas SIP que llegan al puerto 224497 pertenecen a la misma sesión existente.

No obstante, la escucha de muchos puertos en paralelo podría provocar problemas de rendimiento o escalabilidad.

Como alternativa adicional, en el SIP se puede usar un campo de encabezamiento de extensión privativo nuevo para transportar la información oculta. Como ejemplo, el campo nuevo de encabezamiento de extensión puede tener este aspecto:

CSCF-session: "ISId=224497 in scscf17.operador.net"

No obstante, tal como ya se ha mencionado en relación con el primer ejemplo, el UA debería soportar esta característica, es decir, copiar este campo de encabezamiento nuevo desde las solicitudes de SIP a las respuestas SIP y las solicitudes SIP subsiguientes.

Todavía como alternativa adicional, para esta opción también se podría usar la parte de carga útil de la solicitud o respuesta SIP.

Los mecanismos anteriores de compartición de carga se proporcionan principalmente en funciones CSCF u otros nodos de red con una funcionalidad correspondiente. No obstante, en general, los mismos también se pueden implementar en dispositivos terminales, tales como el UE 10.

Debe indicarse que la presente invención no se limita a las formas de realización preferidas descritas anteriormente. La presente invención se puede implementar en cualquier nodo de red que tenga una funcionalidad de control de carga en cualquier red. En particular, se puede usar cualquier campo de encabezamiento o carga útil de cualquier mensaje o datagrama de datos por paquetes. Además, se puede transportar cualquier información utilizable para el control de la carga. De este modo, las formas de realización pueden variar dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método de control de la carga de procesado en una red de datos por paquetes, comprendiendo dicho método las etapas siguientes:

a) fijar una información de control de carga en un campo predeterminado (121 a 12n) de un mensaje;

b) encaminar dicho mensaje en dicha red de datos por paquetes;

c) comprobar dicha información de control de carga sobre la *via* de encaminamiento de dicho mensaje; y

d) seleccionar un recurso de procesado de dicha red de datos por paquetes en respuesta al resultado de dicha etapa de comprobación.

2. Método según la reivindicación 1, en el que dicho campo predeterminado es un subcampo (121 a 12n) de una parte de usuario (120) de un encabezamiento de dirección (100).

3. Método según la reivindicación 1, en el que dicho campo predeterminado es un parámetro *branch* del campo *via* de un mensaje SIP.

4. Método según la reivindicación 3, que comprende además la etapa en la que se copia dicha información de control de carga desde otro campo predeterminado a dicho campo predeterminado.

5. Método según la reivindicación 2, en el que dicho encabezamiento de dirección es un URI (100) de un encabezamiento *Route* SIP.

6. Método según la reivindicación 2 ó 5, que comprende además la etapa en la que se proporciona una pluralidad de subcampos (121 a 12n) en dicha parte de usuario (120) para transportar tipos diferentes de dicha información de control de carga.

7. Método según la reivindicación 6, en el que dicha parte de usuario (120) se analiza sintácticamente y se divide en dicho subcampos (121 a 12n).

8. Método según la reivindicación 6, en el que por lo menos una característica de ente la estructura, el orden y el uso de dichos subcampos (121 a 12n) está predeterminada.

9. Método según cualquiera de las reivindicaciones 6 a 8, en el que dichos subcampos (121 a 12n) se separan mediante una cadena de bits, un carácter, o una cadena de caracteres predeterminados.

10. Método según la reivindicación 1, en el que una pluralidad de nodos procesadores comparte una dirección virtual.

11. Método según la reivindicación 10, en el que dicho nodo procesador tiene una funcionalidad de control del estado de la llamada de una red celular basada en IP.

12. Método según cualquiera de las reivindicaciones 2 a 11, en el que dicha información de control de carga comprende un primer número de puerto que indica un primer puerto para recibir un mensaje de solicitud.

13. Método según cualquiera de las reivindicaciones 2 a 12, en el que dicha información de control de carga comprende un segundo número de puerto que indica un segundo puerto para recibir un mensaje de respuesta.

14. Método según la reivindicación 1, en el que dicha información de control de carga comprende una primera información que indica si ya existe una sesión de dicho mensaje.

15. Método según la reivindicación 14, en el que dicha información de control de carga comprende una segunda información que indica una identificación de dicha sesión existente.

16. Método según la reivindicación 14 ó 15, en el que dicha información de control de carga se almacena en un campo de encabezamiento *Route*, un campo de encabezamiento *Via*, o un campo de encabezamiento *Contact* de un mensaje SIP.

17. Método según cualquiera de las reivindicaciones 14 a 16, en el que dicha información de control de carga es una información oculta sin sentido para otras redes.

18. Método según cualquiera de las reivindicaciones 14 a 17, en el que dicha información de control de carga se fija como parte de un nombre de anfitrión de un campo de encabezamiento.

19. Método según cualquiera de las reivindicaciones 14 a 17, en el que dicha información de control de carga se fija como un parámetro de un campo de encabezamiento.

20. Método según cualquiera de las reivindicaciones 14 a 17, en el que dicha información de control de carga se fija como un número de puerto de un campo de encabezamiento.

21. Método según la reivindicación 20, en el que dicho número de puerto se usa para diferenciar un primer mensaje con respecto a mensajes subsiguientes.

22. Método según cualquiera de las reivindicaciones 14 a 17, en el que dicha información de control de carga se fija como un campo de encabezamiento de extensión para un campo de encabezamiento.

23. Método según cualquiera de las reivindicaciones 14 a 17, en el que dicha información de control de carga se fija en una parte de carga útil de dicho mensaje.

24. Método según la reivindicación 15, que comprende además las etapas en las que se extrae dicha segunda información en respuesta a una detección de dicha primera información, y se usa dicha segunda información para dicha etapa de selección.

25. Método de distribución de información de control de carga en una red por conmutación de paquetes, que comprende las etapas siguientes:

a) crear una primera información de control de carga para seleccionar recursos de procesado de dichas redes de paquetes en un primer elemento de red (20);

b) fijar dicha primera información de control de carga en un campo predeterminado de un mensaje;

c) encaminar dicho mensaje hacia un segundo elemento de red (40);

d) almacenar dicha primera información de control de carga en dicho segundo elemento de red;

e) crear una segunda información de control de carga para seleccionar recursos de procesado de dichas redes de paquetes en dicho segundo elemento de red;

f) fijar dicha segunda información de control de carga en un campo predeterminado de un segundo mensaje;

g) encaminar dicho segundo mensaje hacia dicho primer elemento de red; y

h) almacenar dicha segunda información de control de carga en dicho primer elemento de red.

26. Dispositivo de red para controlar la carga de procesado en una red de datos por paquetes, comprendiendo dicho dispositivo (20, 40):

a) unos medios de comprobación para comprobar una información de control de carga proporcionada en un campo predeterminado (121 a 12n) de un mensaje;

b) unos medios de selección para seleccionar un recurso de procesado para dicho mensaje en respuesta a dichos medios de comprobación.

27. Dispositivo de red según la reivindicación 26, en el que dicho dispositivo de red (20, 40) comprende una funcionalidad de control del estado de la llamada de una red celular basada en IP.

28. Dispositivo de red según la reivindicación 26 ó 27, en el que dichos medios de selección están dispuestos para seleccionar un nodo procesador predeterminado hacia el cual se distribuye dicho mensaje.

29. Dispositivo de red según la reivindicación 26 ó 27, en el que dichos medios de selección están dispuestos para iniciar la creación de una sesión nueva.

30. Dispositivo de red según la reivindicación 29, en el que dicha información de control de carga comprende una primera información que indica si ya existe una sesión de dicho mensaje.

31. Dispositivo de red según la reivindicación 30, en el que dicha información de control de carga comprende una segunda información para identificar dicha sesión existente.

32. Dispositivo para transmitir un mensaje hacia una red de datos por paquetes, estando dispuesto dicho dispositivo (10, 20, 40) para fijar en un campo predeterminado (121 a 12n) de dicho mensaje una información de control de carga para seleccionar recursos de procesado de dicha red de datos por paquetes.

33. Dispositivo según la reivindicación 32, en el que dicho dispositivo comprende una funcionalidad de control del estado de la llamada de una red celular basada en IP.

34. Dispositivo según la reivindicación 33, en el que dicha funcionalidad de control del estado de la llamada es una funcionalidad de control del estado de la llamada de servicio o una funcionalidad *proxy* de control del estado de la llamada.

35. Dispositivo según cualquiera de las reivindicaciones 32 a 34, en el que dicho dispositivo está dispuesto para fijar dicha información de control de carga en una parte de usuario (120) de una dirección de encabezamiento (100) de dicho mensaje.

36. Dispositivo según la reivindicación 35, en el que dicha dirección de encabezamiento es un URI SIP (100).

37. Dispositivo según cualquiera de las reivindicaciones 32 a 34, en el que dicho dispositivo está dispuesto para fijar dicha información de control de carga en un nombre de anfitrión, un parámetro de encabezamiento, un número de puerto, o un campo de encabezamiento de extensión de una parte de encabezamiento de dicho mensaje, o en una parte de carga útil de dicho mensaje.

38. Dispositivo según la reivindicación 37, en el que dicha información de control de carga comprende una primera información que indica si ya existe una sesión de dicho mensaje.

39. Dispositivo según la reivindicación 38, en el que dicha información de control de carga comprende una segunda información que indica dicha sesión existente.

40. Sistema para controlar la carga de procesado en una red de datos por paquetes, comprendiendo dicho sistema:

a) un primer elemento de red (10, 20, 40) dispuesto para fijar una información de control de carga en un campo predeterminado (121 a 12n) de un mensaje a encaminar en dicha red de datos por paquetes; y

b) un segundo elemento de red (20, 40) dispuesto para comprobar dicha información de control de carga sobre la vía de encaminamiento de dicho mensaje; y para seleccionar un recurso de procesado de dicha red de datos por paquetes en respuesta al resultado de la comprobación.

41. Sistema para distribuir información de control de carga en una red por conmutación de paquetes, comprendiendo dicho sistema:

a) un primer elemento de red (20) dispuesto para crear una primera información de control de carga para seleccionar recursos de procesado de dichas redes de datos por paquetes y para fijar dicha primera información de control de carga en un campo predeterminado de un mensaje; y

b) un segundo elemento de red (40) dispuesto para recibir dicho mensaje, para almacenar dicha primera información de control de carga, para crear una segunda información de control de carga, para fijar dicha segunda información de control de carga en un campo predeterminado de un segundo mensaje, y para encaminar dicha segunda información de control de carga hacia dicho primer elemento de red;

c) en el que dicho primer elemento de red (20) está adaptado para almacenar dicha segunda información de control de carga.

42. Sistema según la reivindicación 40 ó 41, en el que dichos primer y segundo dispositivos de red comprenden una funcionalidad de control del estado de la llamada.

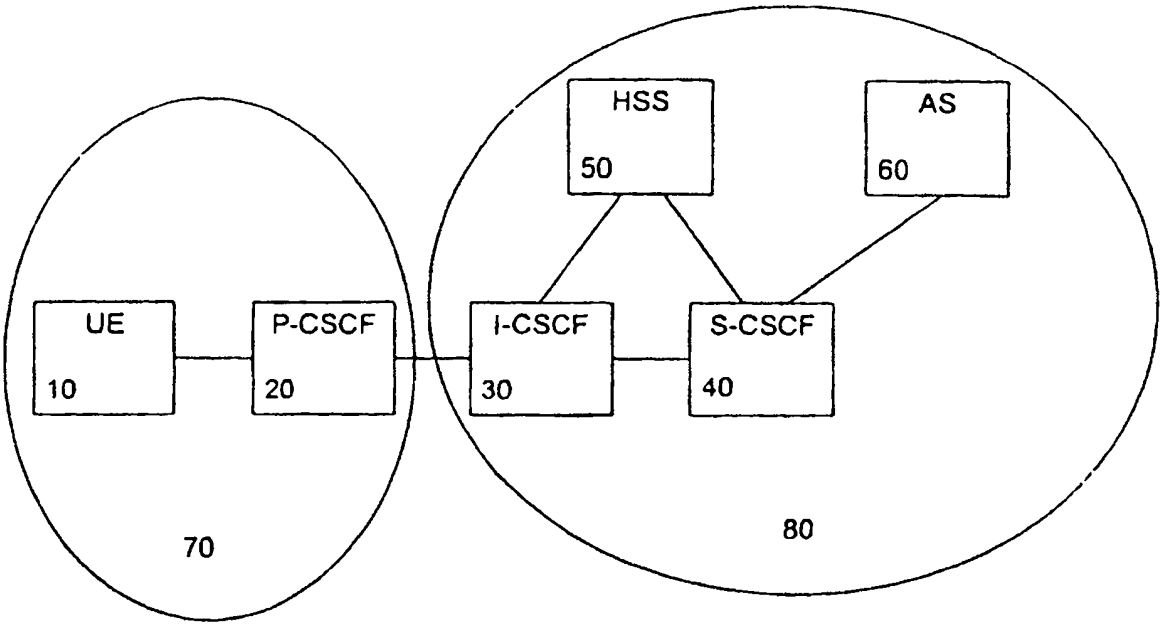
HSS
50
AS
60
UE
10
P-CSCF
20
I-CSCF
30
S-CSCF
40
70
80

Fig. 1

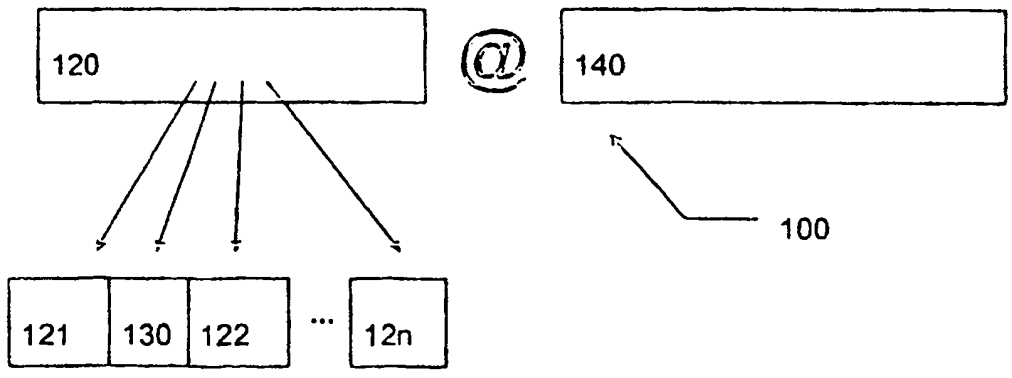
120
@
140
100
121
130
122
...
12n

Fig. 2

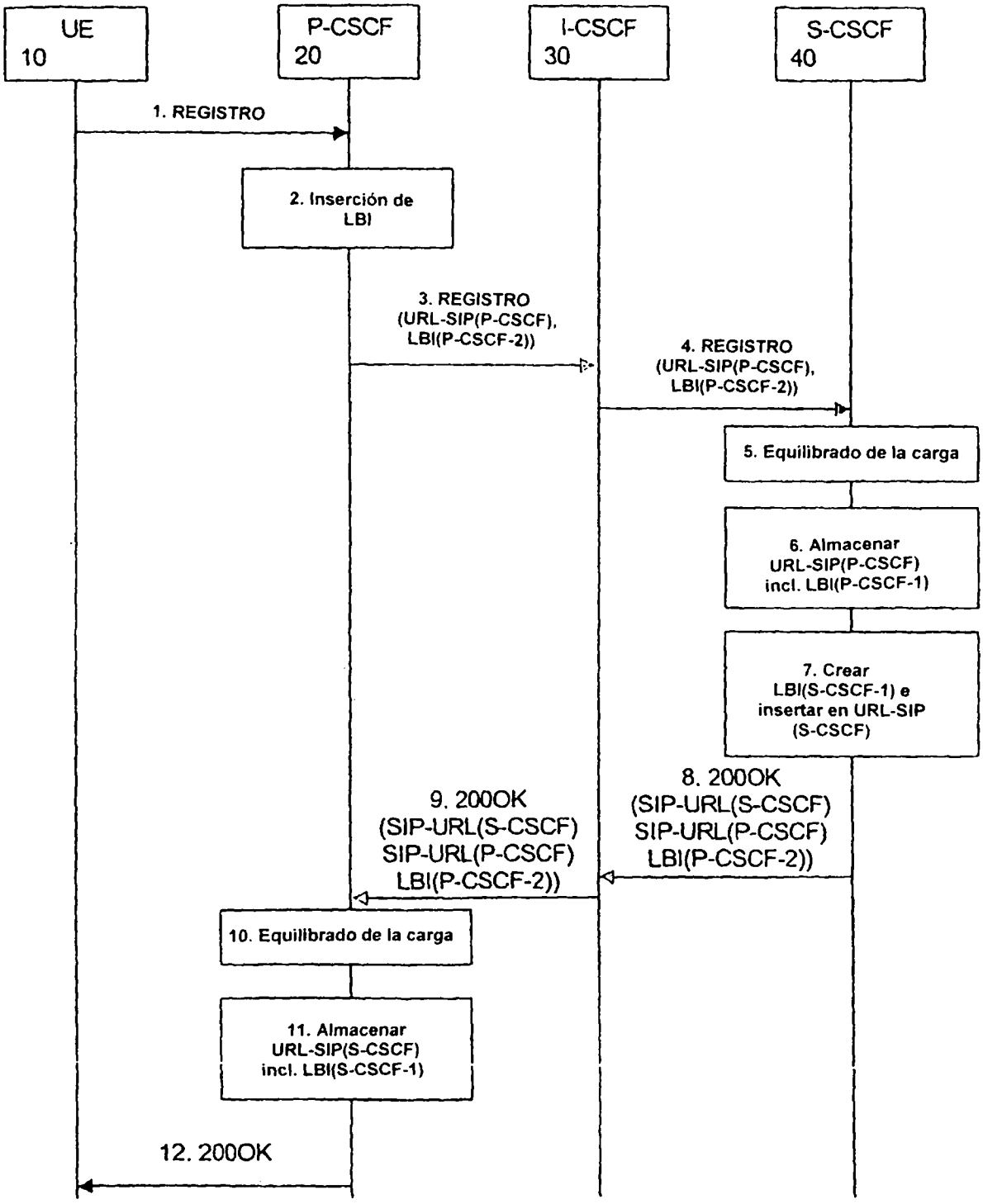
UE
10
P-CSCF
20
I-CSCF
30
S-CSCF
40
1. REGISTRO
2. Inserción de LBI
3. REGISTRO (URL-SIP(P-CSCF), LBI(P-CSCF-2))
4. REGISTRO (URL-SIP(P-CSCF), LBI(P-CSCF-2))
5. Equilibrado de la carga
6. Almacenar URL-SIP(P-CSCF) incl. LBI(P-CSCF-1)
7. Crear LBI(S-CSCF-1) e insertar en URL-SIP (S-CSCF)
8. 200OK (SIP-URL(S-CSCF) SIP-URL(P-CSCF) LBI(P-CSCF-2))
9. 200OK (SIP-URL(S-CSCF) SIP-URL(P-CSCF) LBI(P-CSCF-2))
10. Equilibrado de la carga
11. Almacenar URL-SIP(S-CSCF) incl. LBI(S-CSCF-1)
12. 200OK

Fig. 3

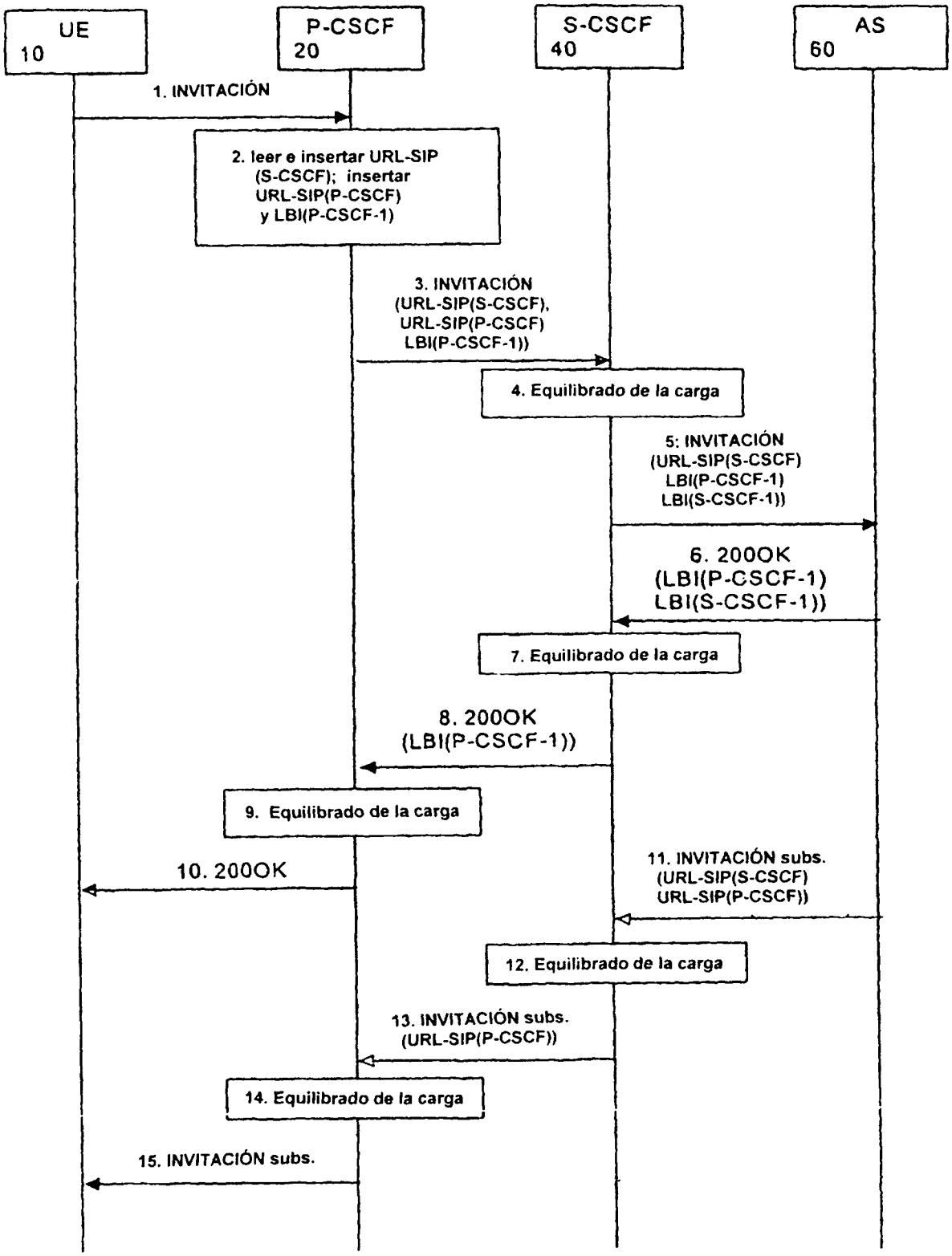
UE
10
P-CSCF
20
S-CSCF
40
AS
60
1. INVITACIÓN
2. leer e insertar URL-SIP (S-CSCF); insertar URL-SIP(P-CSCF) y LBI(P-CSCF-1)
3. INVITACIÓN (URL-SIP(S-CSCF), URL-SIP(P-CSCF) LBI(P-CSCF-1))
4. Equilibrado de la carga
5: INVITACIÓN (URL-SIP(S-CSCF) LBI(P-CSCF-1) LBI(S-CSCF-1))
6. 200OK (LBI(P-CSCF-1) LBI(S-CSCF-1))
7. Equilibrado de la carga
8. 200OK (LBI(P-CSCF-1))
9. Equilibrado de la carga
10. 200OK
11. INVITACIÓN subs. (URL-SIP(S-CSCF) URL-SIP(P-CSCF))
12. Equilibrado de la carga
13. INVITACIÓN subs. (URL-SIP(P-CSCF))
14. Equilibrado de la carga
15. INVITACIÓN subs.

Fig. 4

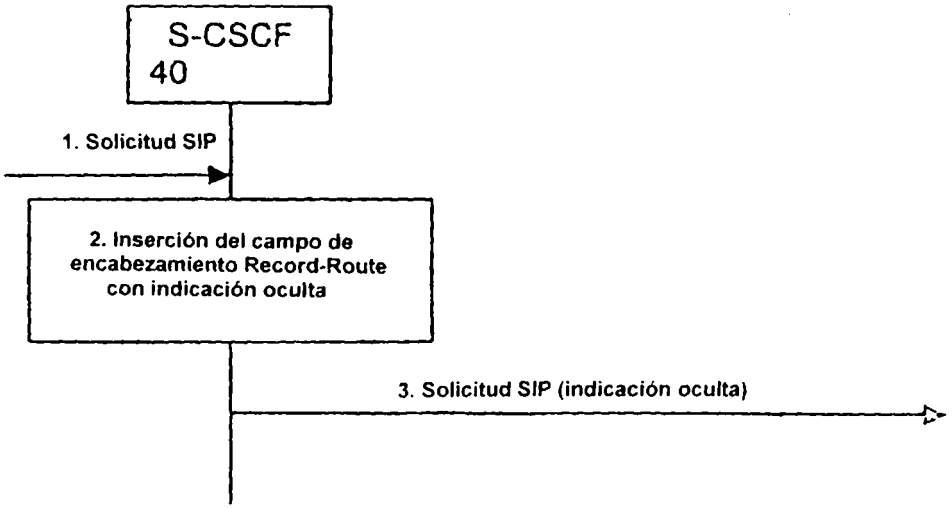
S-CSCF
40
1. Solicitud SIP
2. Inserción del campo de encabezamiento Record-Route con indicación oculta
3. Solicitud SIP (indicación oculta)

Fig. 5

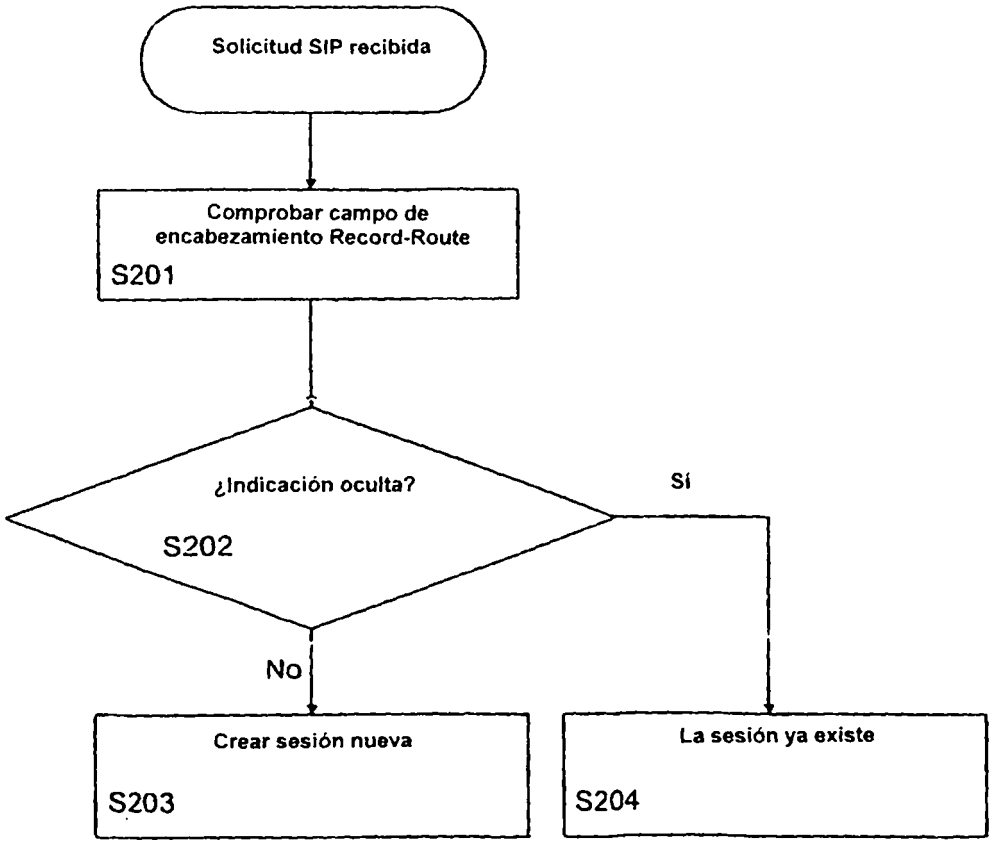
Solicitud SIP recibida
Comprobar campo de encabezamiento Record-Route
S201
¿Indicación oculta?
S202
Sí
No
Crear sesión nueva
S203
La sesión ya existe
S204

Fig. 6

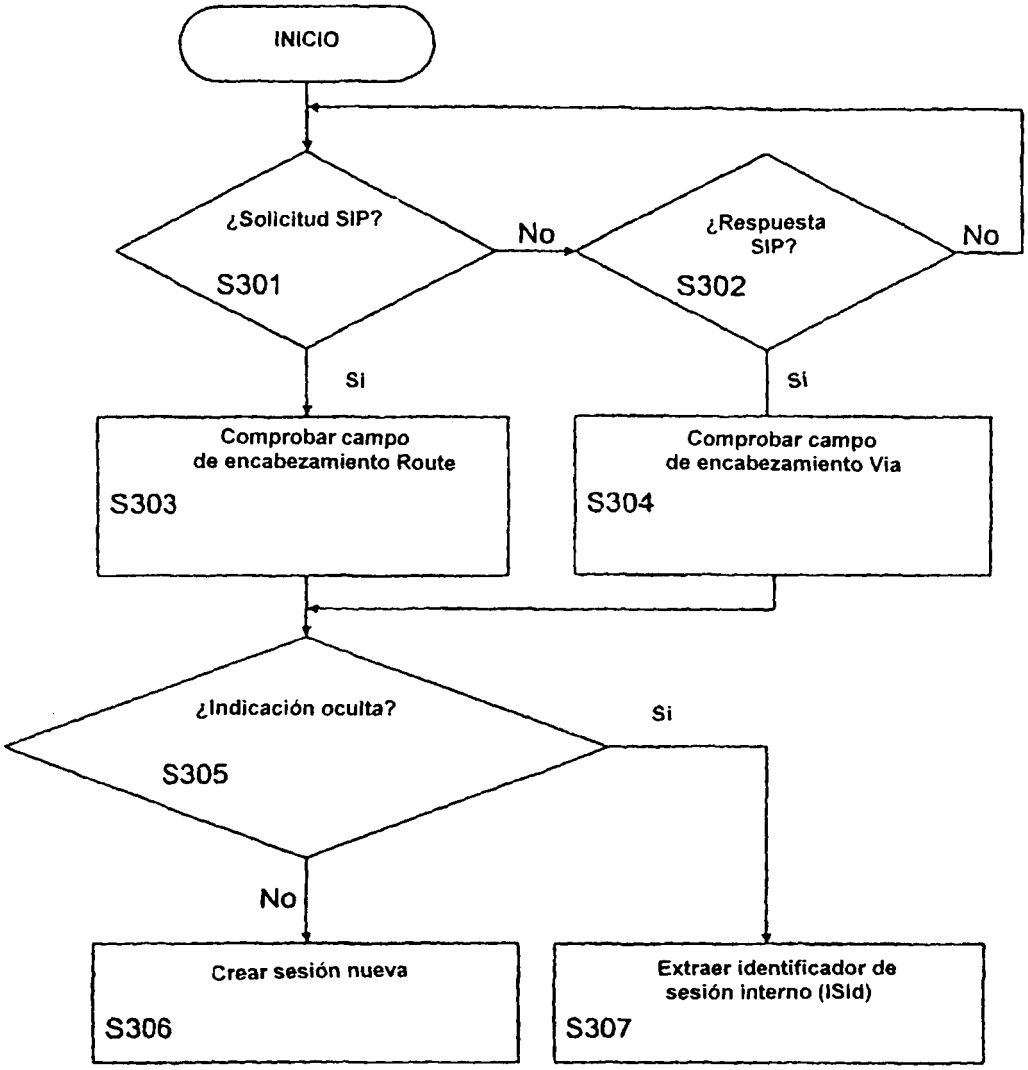
INICIO
¿Solicitud SIP?
S301
No
¿Respuesta SIP?
S302
No
Sí
Sí
Comprobar campo de encabezamiento Route
S303
Comprobar campo de encabezamiento Via
S304
¿Indicación oculta?
S305
Sí
No
Crear sesión nueva
S306
Extraer identificador de sesión interno (ISId)
S307

Fig. 7