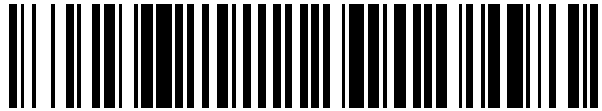


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 401 301**

51 Int. Cl.:

H04L 29/14 (2006.01)

H04L 29/12 (2006.01)

H04L 29/08 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **19.12.2007 E 07857812 (7)**

97 Fecha y número de publicación de la concesión europea: **12.12.2012 EP 2223500**

54 Título: **Método y aparato para su uso en una red de comunicaciones**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
18.04.2013

73 Titular/es:

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

72 Inventor/es:

LAFUENTE ALVAREZ, LUIS, MARIA;
CELAYA PRIETO, ALFONSO y
PEREZ FERNANDEZ, JAVIER

74 Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

ES 2 401 301 T3

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

DESCRIPCIÓN

Método y aparato para su uso en una red de comunicaciones.

5 Campo técnico
 La presente invención se refiere a un método y aparato para su uso en una red de comunicaciones, por ejemplo un Sistema Universal de Telecomunicaciones Móvil que tiene un Subsistema Multimedia IP.

Antecedentes

10 Los servicios Multimedia IP proporcionan una combinación dinámica de voz, vídeo, mensajería, datos, etc. dentro de la misma sesión. Mediante el aumento del número de aplicaciones básicas y los medios que es posible combinar, crecerá el número de servicios ofrecido a los usuarios finales, y se enriquecerá la experiencia de comunicación inter personal. Esto conducirá a una nueva generación de servicios de comunicación multimedia ricos, personalizados, incluyendo los denominados servicios "Multimedia IP combinacionales".

15 El UMTS (Sistema Universal de Telecomunicaciones Móviles) es un sistema inalámbrico de tercera generación diseñado para proporcionar tasas de datos mayores y servicios mejorados a los abonados. El UMTS es un sucesor del Sistema Global para Comunicaciones Móviles (GSM), con un importante paso evolutivo entre GSM y UMTS que es el Servicio General de Radio por Paquetes (GPRS). El GPRS introduce la conmutación por paquetes dentro de la red central de GSM y permite acceso directo a las redes de datos por paquetes (PDN). Esto permite transmisiones de conmutación por paquetes de alta tasa de datos mucho más allá del límite de 64 kbps de ISDN a través de la red de llamadas GSM, que es una necesidad para tasas de transmisión de datos UMTS de hasta 2 Mbps. El UMTS está estandarizado por el Proyecto de Cooperación de 3ª Generación (3GPP) que es un conglomerado de órganos de estándares regionales tales como el Instituto Europeo de Estándares de Telecomunicación (ETSI), la Asociación de Empresas de la Industria de la Radio (ARIB) y otros. Ver la TS 23.002 del 3GPP para más detalles.

20 La arquitectura UMTS incluye un subsistema conocido como el Subsistema Multimedia IP (IMS) para soportar telefonía tradicional así como nuevos servicios multimedia IP (TS 22.228, TS 23.228, TS 24.229, TS 29.228, TS 29.229, TS 29.328 y TS 29.329 del 3GPP Publicaciones 5 a 7). El IMS proporciona rasgos clave para enriquecer la experiencia de comunicación persona a persona del usuario final a través del uso de Habilitadores del Servicio IMS estandarizados, que facilitan nuevos servicios de comunicación persona a persona (cliente a cliente) ricos así como servicios persona a contenido (cliente a servidor) sobre redes basadas en IP. El IMS es capaz de conectar tanto con PSTN/ISDN (Red Telefónica Pública Conmutada/Red Digital de Servicios Integrados) así como con Internet.

35 El IMS hace uso del Protocolo de Inicio de Sesiones (SIP) para configurar y controlar llamadas o sesiones entre terminales de usuario (o terminales de usuario y servidores de aplicaciones). El Protocolo de Descripción de Sesiones (SDP), transportado mediante señalización SIP, se usa para describir y negociar los componentes de medios de la sesión. Mientras que SIP fue creado como un protocolo de usuario a usuario, IMS permite a los operadores y proveedores de servicios controlar el acceso de usuario a los servicios y cargar a los usuarios en consecuencia. El 3GPP ha elegido SIP para señalización entre un Equipo de Usuario (UE) y el IMS así como entre los componentes dentro del IMS.

40 Detalles específicos de la operación de la red de comunicaciones UMTS y los diversos componentes dentro de tal red se pueden encontrar en las Especificaciones Técnicas para UMTS que están disponibles en <http://www.3gpp.org>. Detalles adicionales del uso de SIP dentro de UMTS se pueden encontrar en la Especificación Técnica TS 24.228 V5.8.0 (2004-03) del 3GPP.

45 La Figura 1 de los dibujos anexos ilustra esquemáticamente cómo el IMS encaja en la arquitectura de red móvil en el caso de una red de acceso GPRS/PS (IMS puede operar por supuesto sobre otras redes de acceso). Las Funciones de Control de Llamadas/Sesiones (CSCF) operan como intermediarios SIP dentro del IMS. La arquitectura 3GPP define tres tipos de CSCF: la CSCF Intermediaria (P-CSCF) que es el primer punto de contacto dentro del IMS para un terminal SIP; la CSCF de Servicio (S-CSCF) que proporciona servicios al usuario a los que está suscrito el usuario; y la CSCF de Interrogación (I-CSCF) cuyo papel es identificar la S-CSCF correcta y reenviar a esa S-CSCF una petición recibida desde un terminal SIP a través de una P-CSCF.

55 Un usuario se registra con el IMS usando el método SIP REGISTER especificado. Este es un mecanismo para unirse al IMS y anunciar al IMS la dirección a la que se puede alcanzar una identidad de usuario SIP. En el 3GPP, cuando un terminal SIP realiza un registro, el IMS autentifica el usuario, y asigna una S-CSCF a ese usuario a partir del conjunto de S-CSCF disponibles. Mientras que el criterio para asignar las S-CSCF no se especifica por el 3GPP, estas pueden incluir compartición de carga y requerimientos de servicio. Se señala que la asignación de una S-CSCF es clave para controlar (y para cargar) el acceso de usuario a servicios basados en IMS. Los operadores pueden proporcionar un mecanismo para impedir sesiones SIP de usuario a usuario directas que de otro modo desviarían la S-CSCF.

- 5 Durante el proceso de registro, es responsabilidad de la I-CSCF seleccionar una S-CSCF si no está ya seleccionada una S-CSCF. La I-CSCF recibe las capacidades de la S-CSCF requeridas desde el Servidor de Abonado Residencial (HSS) de la red, y selecciona una S-CSCF adecuada en base a las capacidades recibidas. (Se señala que la asignación de la S-CSCF también se lleva a cabo para un usuario por la I-CSCF en el caso donde el usuario es llamado por otra parte, y no está asignada actualmente al usuario una S-CSCF.) Cuando un usuario registrado envía posteriormente una petición de sesión al IMS, la P-CSCF es capaz de reenviar la petición a la S-CSCF seleccionada en base a la información recibida desde la S-CSCF durante el proceso de registro.
- 10 Dentro de la red de servicio del IMS, los Servidores de Aplicaciones (AS) se proporcionan para implementar la funcionalidad de servicio del IMS. Los Servidores de Aplicaciones proporcionan servicios a los usuarios finales en un sistema IMS, y pueden estar conectados o bien como puntos finales sobre el interfaz Mr definida por el 3GPP, o bien “enlazados” por una S-CSCF sobre la interfaz ISC definida del 3GPP. En este último caso, los Criterios de Filtro Inicial (IFC) se usan por una S-CSCF para determinar qué Servidores de Aplicaciones deberían estar “enlazados” durante un establecimiento de Sesión SIP. Se pueden aplicar diferentes IFC a diferentes casos de llamada. Los IFC se reciben por la S-CSCF desde un HSS durante el procedimiento de registro del IMS como parte de un Perfil de Usuario del usuario. Ciertos Servidores de Aplicaciones realizan acciones dependientes de las identidades de abonado (o bien el abonado llamado o el que llama, lo que es “propiedad” de la red que controla el Servidor de Aplicaciones). Por ejemplo, en el caso de desvío de llamadas, el servidor de aplicaciones adecuado (de terminación) determinará la nueva parte de terminación a la que será reenviada una llamada a un abonado dado. En el caso de que un IFC indique que un mensaje SIP recibido en la S-CSCF se debería reenviar a un AS de SIP particular, ese AS se añade dentro del trayecto del mensaje. Una vez que el mensaje SIP se devuelve por el AS a la S-CSCF, se reenvía hacia su destino final, o reenvía a otro AS si esto se indica en los IFC.
- 15 Como se mencionó anteriormente, en una red IMS, el HSS está a cargo principalmente de almacenar los datos de abonado. El HSS interactúa con otros nodos (conocidos en la presente memoria de manera general como “clientes HSS”) por medio del protocolo Diámetro (RFC 3588). Ejemplos de tal cliente HSS son la I-CSCF, la S-CSCF, el AP (Intermediario de Agregación) y el AS (Servidor de Aplicaciones).
- 20 La intención general es que el HSS sea una base de datos central para un dominio. No obstante, algunas redes tienen más usuarios que se pueden manejar por un único HSS, y estas redes por lo tanto se dotan con más de un HSS. Las redes con más de un HSS también contienen una Función de Ubicación de Suscripción (SLF). Los nodos que necesitan consultar a un HSS sobre un usuario particular primero consultan la SLF, la cual devuelve la dirección del HSS que maneja el usuario. La SLF esencialmente actúa como un agente de redirección de Diámetro.
- 25 No obstante, el escenario autónomo, solamente con un HSS y ninguna SLF desplegada en la red, es muy común en despliegues actuales y también se debe considerar.
- 30 La lógica de encaminamiento de Diámetro que implica el HSS se puede encontrar en la TS 29.228 del 3GPP. Aunque los siguientes extractos se centran en nodos CSCF, aplican igualmente a cualquier otro tipo de cliente HSS.
- 35 “Si una I-CSCF o S-CSCF conoce la dirección/nombre del HSS para un cierto usuario, tanto las AVP (Parejas de Valores de Atributo) del Campo de Destino como del Ordenador Principal de Destino deberán estar presentes en la petición. De otro modo, solamente estará presente la AVP del Campo de Destino y el comando se encaminará al siguiente nodo de Diámetro, por ejemplo la SLF, en base a la tabla de encaminamiento de Diámetro en el cliente.
- 40 Una vez que la función de redirección (SLF) ha devuelto la dirección o el HSS destino (usando la AVP del Ordenador Principal de Redirección), la petición redirigida al HSS incluirá tanto las AVP del Campo de Destino como del Ordenador Principal de Destino.
- 45 La S-CSCF almacena la dirección del HSS para cada usuario, después de que una primera petición se envió a la función de redirección.
- 50 Las peticiones iniciadas por el HSS hacia una S-CSCF incluirán tanto las AVP del Ordenador Principal de Destino como del Campo de Destino. El HSS obtiene la AVP del Ordenador Principal de Destino para usar en peticiones hacia una S-CSCF, a partir de la AVP del Ordenador Principal de Origen recibida en peticiones previas desde la S-CSCF. Por consiguiente, la AVP del Ordenador Principal de Destino se declara como obligatoria en la ABNF para todas las peticiones iniciadas por el HSS.
- 55 La AVP del Campo de Destino se declara como obligatoria en la ABNF para todas las peticiones.”
- 60 Como se aprecia por el solicitante, un asunto que no está específicamente abordado en el estándar del 3GPP es aquél de una solución de redundancia para el HSS: en un despliegue real los datos de usuario se podrían almacenar en más de un HSS (por ejemplo en una configuración en caliente/espera activa, que es la actualmente disponible en el TSP, compartición de carga, y demás). Un mecanismo que permitiría a un cliente HSS aprender la dirección del HSS correcta no se especifica en el estándar del 3GPP. El documento de Diámetro (RFC3588) del IETF proporciona
- 65

- 5 una solución de redundancia para “agentes de Diámetro” pero no para ordenadores principales de destino. Por ejemplo, en IMS del 3GPP una Función de Ubicación de Suscripción (SLF) es un “agente de redirección de Diámetro”, y un Servidor de Abonado Residencial HSS es un ordenador principal de destino (ver por ejemplo el documento “User identity to HSS resolution”, Ericsson, Borrador del 3GPP; N4-020160, Proyecto de Cooperación de 3ª Generación, Centro de Competencia Móvil; 650, Route des Lucioles; F-06921 Sophia-Antipolis Cedex; Francia, nº Sophia; 20020128, 24 de enero de 2002, XP050080118, el cual describe el uso de múltiples HSS para proporcionar capacidad adicional).
- 10 Es deseable abordar este asunto.
- 15 Compendio
Según un primer aspecto de la presente invención hay proporcionado un método según la reivindicación 1 para permitir redundancia para un Servicio de Abonado Residencial, HSS, de un Subsistema Multimedia IP, IMS, con la redundancia que se proporciona por una pluralidad de casos de HSS, donde los datos para cada uno de la pluralidad de usuarios se gestionan por más de uno de los casos de HSS, y el método que comprende: donde un nodo cliente del IMS requiere detalles de un HSS, disponer el nodo cliente para ser dotado con detalles de un HSS intermediario que representa los casos de HSS; y disponer el HSS intermediario para: seleccionar uno adecuado de los casos de HSS para manejar una petición recibida en el HSS intermediario desde el nodo cliente; cambiar una Pareja de Valores de Atributos del ordenador principal destino en la petición recibida en base a la selección; y reenviar la petición al caso de HSS seleccionado para la manipulación.
- 20 El método puede comprender, donde se proporcione una Función de Ubicación de Suscripción, SLF, en el IMS, disponer la SLF para dotar al nodo cliente con detalles del HSS intermediario.
- 25 El método puede comprender, donde no se proporcione una Función de Ubicación de Suscripción, SLF, en el IMS, disponer el HSS intermediario en sí mismo para dotar al nodo cliente con detalles del HSS intermediario.
- 30 El protocolo de Diámetro se puede usar para comunicación entre el nodo cliente y el HSS intermediario.
- 35 La redundancia del HSS intermediario también se puede dotar, teniendo una pluralidad de casos de HSS intermediario, con redundancia hacia los casos de HSS intermediario que se manejan mediante mecanismos de protocolo de Diámetro estándar.
- Al menos algunos de los casos de HSS pueden ser diferentes circuitos de entrada respectivos a una base de datos.
- El método puede comprender mantener información en el HSS intermediario para su uso en realizar la selección.
- 40 La información puede comprender al menos uno de: información relativa a las cargas respectivas que se experimentan por los casos de HSS; disponibilidades respectivas de los casos de HSS; y estados respectivos de los casos de HSS.
- Donde la base de datos esté distribuida a través de una pluralidad de emplazamientos, la información puede comprender información geográfica relativa a los emplazamientos.
- 45 El método puede comprender monitorizar el estado de cada caso de HSS para su uso en realizar la selección.
- El método puede comprender monitorizar el estado usando mensajes de Diámetro.
- 50 El método puede comprender monitorizar el estado usando mensajes DWR/DWA.
- El método puede comprender realizar la selección en base a al menos uno de ubicación geográfica, disponibilidad, carga, y tiempo de respuesta.
- 55 El HSS intermediario puede ser un nodo del IMS.
- El HSS intermediario puede ser un agente intermediario de Diámetro.
- El nodo cliente puede ser un cliente de Diámetro.
- 60 El nodo cliente puede comprender al menos uno de: una Función de Control de Sesión de Llamada de Interrogación del IMS, una Función de Control de Sesión de Llamada de Servicio del IMS; un Intermediario de Agregación del IMS; y un Servidor de Aplicaciones del IMS.
- 65 El método se puede realizar en el HSS intermediario.

El HSS se puede sustituir por un ordenador principal de destino del IMS distinto de un HSS.

5 Según un segundo aspecto de la presente invención hay proporcionado un aparato según la reivindicación 16 para permitir redundancia para un Servicio de Abonado Residencial, HSS, de un Subsistema Multimedia IP, IMS, con redundancia que se proporciona por una pluralidad de casos de HSS, donde los datos para cada uno de la pluralidad de usuarios se gestionan por más de uno de los casos de HSS, y el aparato que comprende: medios para disponer, donde un nodo cliente del IMS requiera detalles de un HSS, para que el nodo cliente sea dotado con detalles de un HSS intermediario que representa los casos de HSS; y medios para disponer el HSS intermediario para: seleccionar uno adecuado de los casos de HSS para manejar una petición recibida en el HSS intermediario desde el nodo cliente; cambiar una Pareja de Valores de Atributos de ordenador principal destino en la petición recibida en base a la selección; y reenviar la petición al caso de HSS seleccionado para la manipulación.

El aparato puede comprender el HSS intermediario.

15 Según otro aspecto de la presente invención hay proporcionado un programa y medio de almacenamiento según las reivindicaciones 18 y 19.

20 Según otro aspecto de la presente invención hay proporcionado un método de habilitar redundancia para un ordenador principal de destino de un Subsistema Multimedia IP, IMS, con la redundancia que se proporciona por una pluralidad de casos de ordenador principal de destino, y el método que comprende: donde un nodo cliente del IMS requiera detalles de un ordenador principal de destino, disponer el nodo cliente para ser dotado con detalles de un ordenador principal de destino intermediario que representa los casos de ordenador principal de destino; disponer el ordenador principal de destino intermediario para seleccionar uno adecuado de los casos de ordenador principal de destino para manejar una petición recibida en el ordenador principal de destino intermediario desde el nodo cliente; y disponer el ordenador principal de destino intermediario para reenviar la petición al caso de ordenador principal de destino seleccionado para la manipulación. El ordenador principal de destino intermediario puede ser un agente intermediario de Diámetro. También se proporciona el aparato que comprende los medios para realizar estos pasos del método.

30 Un método para habilitar redundancia para un servidor de protocolos de una red de comunicación, con la redundancia que se proporciona por una pluralidad de casos de servidor de protocolos, y el método que comprende: donde un cliente de protocolo requiera detalles de un servidor de protocolos, disponer el cliente de protocolo para ser dotado con detalles de un servidor de protocolos intermediario que representa los casos de servidor de protocolos; disponer el servidor de protocolos intermediario para seleccionar uno adecuado de los casos de servidor de protocolos para manejar una petición recibida en el servidor de protocolos intermediario desde el cliente de protocolo; y disponer el servidor de protocolo intermediario para reenviar la petición al caso del servidor de protocolos seleccionado para la manipulación. El protocolo puede ser el protocolo de Diámetro. El servidor de protocolos intermediario puede ser un agente intermediario de Diámetro. También se proporciona el aparato que comprende los medios para realizar estos pasos del método.

40 Según un tercer aspecto de la presente invención hay proporcionado un programa para controlar un aparato para realizar un método según el primer aspecto de la presente invención o que, cuando se carga en un aparato, hace al aparato llegar a ser un aparato según el segundo aspecto de la presente invención. El programa se puede realizar en un medio portador. El medio portador puede ser un medio de almacenamiento. El medio portador puede ser un medio de transmisión.

Según un cuarto aspecto de la presente invención hay proporcionado un aparato programado por un programa según el tercer aspecto de la presente invención.

50 Según un quinto aspecto de la presente invención hay proporcionado un medio de almacenamiento que contiene un programa según el tercer aspecto de la presente invención.

Una realización de la presente invención tiene al menos una de las siguientes ventajas:

55 Como hay un HSS lógico desplegado en la red, es posible para cualquier producto de terceros suministradores tomar ventaja de la solución de redundancia del HSS (que no está estandarizada). La interfaz entre el cliente HSS y la aplicación intermediaria de Diámetro se basa en puros mecanismos estándar de Diámetro.

60 No son necesarios cambios en las tablas de encaminamiento IP, y, ventajosamente, los nodos cliente solamente necesitan ser configurados con la dirección de destino del aparato Intermediario en una realización de la presente invención, que se dispone para sustituir la dirección de destino recibida desde un nodo cliente, la cual direcciona el aparato Intermediario, en una dirección de destino del servidor seleccionado allí dentro.

65 La lógica de distribución al par de destino se puede configurar dependiendo del escenario: se puede basar en compartición de carga, ubicación de usuario...

Son válidos un método y aparato para realizar la presente invención tanto para, las arquitecturas de HSS "monolítico" actual como la de HSS de niveles (de capas). No importa si el destino final es un HSS monolítico o un Circuito de Entrada.

5 Breve descripción de los dibujos
 La Figura 1, tratada anteriormente, ilustra esquemáticamente la integración de un Subsistema Multimedia IP en un sistema de comunicaciones móviles 3G;
 10 La Figura 2 es un diagrama de flujo esquemático que ilustra los pasos realizados en una realización de la presente invención;
 La Figura 3 es un diagrama de bloques esquemático que muestra partes del aparato que realiza la presente invención para realizar el método de la Figura 2;
 La Figura 4 es un diagrama de bloques esquemático que muestra el uso de múltiples HSS intermediarios (Intermediarios de Diámetro) en un sistema que realiza la presente invención; y
 15 La Figura 5 es un diagrama de bloques esquemático que muestra partes de un HSS intermediario ejemplo con información que se monitoriza para su uso en la selección de un caso de HSS (circuito de entrada del HSS).

20 Descripción detallada

Se ha mencionado anteriormente que el problema de una solución de redundancia para el HSS no se aborda específicamente en el estándar del 3GPP. Antes de una descripción detallada de una realización de la presente invención, se describirán ahora a su vez las siguientes tres posibles soluciones que abordarían este problema de redundancia, cada una que tiene algunas limitaciones como se expone más adelante: (a) encaminar todo el tráfico a través de la SLF; (b) confiar en procedimientos del estándar de protocolo de Diámetro; y (c) soluciones basadas en capa IP. Esto será seguido por una descripción de: (d) otros mecanismos para obtener el nodo redundante; y entonces (e) una solución según una realización de la presente invención.

25 (a) Encaminar todo el tráfico a través de la SLF

La SLF podría monitorizar el estado del HSS (esto se hace actualmente en el producto IPWorks de Ericsson, para la funcionalidad de DNS del AS, donde se usan SNMP y ICMP para este propósito) y solamente el "activo"/"preferido" se incluiría en las respuestas. Todo el tráfico hacia el HSS se debería encaminar a través de la SLF.

No obstante, según el estándar no es obligatorio para un cliente HSS sondear la SLF siempre que tiene que ser enviado un mensaje al HSS. Algunos ejemplos que se pueden encontrar en implementaciones actuales son:

- La S-CSCF almacena el "ordenador principal de destino" del HSS cuando se recibe desde la SLF la primera vez que se contacta. Desde ese momento en, y para el mismo usuario, se podría mantener esa dirección. No se necesitan sondeos adicionales.
- El ordenador principal de destino del HSS también se puede enviar desde la I-CSCF a la S-CSCF por medio de un mecanismo propietario (integrado en el mensaje SIP REGISTER). En este sentido la S-CSCF no necesita recuperar ninguna información de la SLF, dado que la I-CSCF la ha recibido de la SLF y pasado a la S-CSCF. Esta implementación se usa en las CSCF de Ericsson.

Además, los despliegues actuales no incluyen una SLF cuando el número de abonados es relativamente pequeño; esto significa que también se debe considerar el "escenario de HSS único".

35 (b) Confiar en procedimientos estándar de protocolo de Diámetro

No es posible confiar en puros mecanismos de Diámetro estándar (ver capítulo 5.5.4 de la RFC 3588) dado que son aplicables mecanismos de encaminamiento y conmutación por fallo solamente para escenarios con Agentes de Diámetro a cargo del encaminamiento de los correspondientes mensajes basados en aplicaciones de Diámetro. En este sentido, el mecanismo de conmutación por fallo proporciona una forma alternativa para alcanzar un Ordenador Principal de Destino dado, usando un agente de Diámetro alternativo. Si el ordenador principal de destino como tal está caído, no hay mecanismo especificado en la RFC. Ese sería otro caso.

55 Un Agente de Diámetro es un nodo de Diámetro que proporciona servicios de retransmisión, intermediación, redirección o traducción (realiza la traducción de protocolo entre Diámetro y otro protocolo de AAA). En otras palabras, se usan para encaminar mensajes de Diámetro al destino final (especificado por el ordenador principal de destino).

60 (c) Soluciones basadas en capa IP

Otro planteamiento sería confiar en la capa IP: si los nodos redundantes compartían la misma dirección IP (esto funcionaría para soluciones de redundancia en caliente/espera activa; solamente el nodo "activo" poseería la dirección IP compartida) sería posible ejecutar la conmutación por fallo sin impacto en las aplicaciones. Esta alternativa se ofrece actualmente por el TSP, y también se puede encontrar en otras plataformas comerciales (tal

como por ejemplo el Servidor de Comunicación TCA Avanzado de Motorola; las agrupaciones de Sun también incluyen este rasgo en muchos productos), pero tiene varias desventajas:

- 5 • Tener una IP que se mueve de un sitio a otro implica que la parte de la IP del ordenador principal de las tablas de encaminamiento requerirán algunas actualizaciones en caso de fallo del nodo (se podría usar OSPF para este propósito). Si la troncal está compuesta de muchos encaminadores (router) el encaminamiento del tráfico al destino adecuado no se asegurará hasta que se logre una convergencia de la troncal completa. Se pudiera requerir alguna sintonización de la troncal en cada instalación.
- 10 • Como la troncal está compartida normalmente entre diferentes soluciones los cambios en ella podrían afectar a otras soluciones. De esta manera algunos operadores podrían no estar de acuerdo en tener que hacer tal sintonización. Además el coste de despliegue aumentaría exponencialmente.
- Ésta se percibe como no segura.

(d) Otros mecanismos para obtener el nodo redundante

15 El nodo redundante se podría configurar estáticamente en una tabla. Para cada Ordenador Principal de Destino del HSS posible en la red se manifiesta su secundario (redundante) correspondiente. El cliente HSS entonces podría monitorizar el estado del HSS, y cuando el HSS primario falla, entonces enviaría las consultas de Diámetro al HSS secundario configurado. Una desventaja de esta alternativa es que la redundancia del HSS solamente funcionará en un escenario donde todos los clientes del HSS en la red (la CSCF, los Servidores de Aplicaciones, el servidor de AAA, la BSF, etc.) implementen este mecanismo.

20 Alternativamente, se podría añadir una nueva AVP que transporta información acerca de los nodos redundantes en las respuestas de la SLF. Esto está ahora bajo investigación en el grupo de trabajo DIME del IETF. Una desventaja de esta solución es que estas AVP son opcionales (para proporcionar compatibilidad hacia atrás) y por lo tanto no es posible asegurar que el cliente hará uso de ellas. Además, se necesita la SLF para proporcionar esta información y no es posible encaminar el mensaje en base a otras consideraciones (la ubicación del usuario, el balanceo de carga, y demás).

(e) Una realización de la presente invención

30 En una realización de la presente invención se introduce un intermediario de Diámetro mejorado para proporcionar un HSS lógico único en la red. Se proporcionarán detalles adicionales más adelante, pero en resumen:

- 35 • Cada cliente HSS se puede configurar con un ordenador principal de destino del HSS, y no sería necesaria entonces la SLF (aunque también se puede usar una realización de la presente invención donde una SLF está en operación).
- El punto de acceso al HSS lógico único podría comprometer uno o varios intermediarios de Diámetro mejorados, con cada mensaje de Diámetro enviado desde el cliente HSS que se recibe en uno de estos intermediarios. Desde el lado del cliente HSS, los intermediarios de Diámetro se pueden configurar como en la interfaz de Diámetro estándar.
- 40 • Para proporcionar redundancia y para escalar la capacidad de procesamiento de tráfico, podría haber varios intermediarios. La redundancia hacia los intermediarios se puede lograr con procedimientos estándar de Diámetro (ver RFC 3588 capítulo 5.5.4).
- El intermediario de Diámetro mejorado proporcionaría mecanismos para encontrar cuál es el par de Diámetro más adecuado para procesar el mensaje de Diámetro. Estos pares pueden ser Circuitos de Entrada (FE) del HSS que acceden a una base de datos que contiene datos de usuario, o HSS monolíticos que mantienen tanto la lógica de aplicaciones del HSS como los datos de usuario. Estos mecanismos consideran el HSS monolítico de disponibilidad de FE, la ubicación geográfica de los datos de usuario así como la gestión de la distribución de carga hacia los pares de Diámetro.

50 Una realización de la presente invención se describirá ahora en más detalle con referencia a las Figuras 2 y 3. La Figura 2 es un diagrama de flujo esquemático que ilustra los pasos realizados en una realización de la presente invención, mientras que la Figura 3 es un diagrama de bloques esquemático que muestra partes de un aparato que realiza la presente invención.

55 La Figura 2 muestra un cliente HSS 10 y una SLF 30, los cuales se han descrito previamente. Un HSS en este ejemplo se proporciona con un grado de redundancia comprendiendo un primer y segundo casos de HSS 40. Finalmente, también se proporciona un HSS intermediario 20, cuya función llegará a ser evidente a partir de la descripción de más adelante.

60 En respuesta a una petición por el Cliente HSS 10 de detalles (por ejemplo una "AVP del Ordenador Principal de Destino") de un HSS relativo a un usuario particular, en el paso S1 se proporcionan detalles del HSS intermediario 20 al cliente HSS 10, o bien desde la SLF 30 (si hay una) o (por ejemplo si no hay una SLF) se configuran de antemano en el cliente HSS 10, o se proporcionan desde el HSS intermediario 20 en sí mismo. Ventajosamente, todo cliente HSS 10 está configurado con un Ordenador Principal de Destino del HSS único que direcciona el HSS intermediario 20, el cual proporciona una configuración simplificada de clientes y, al mismo tiempo, permite

prescindir de la necesidad de una SLF. Los detalles del HSS intermediario 20 se reciben por el cliente del HSS 10 en el paso S2.

5 En el paso S3 el cliente HSS 10 envía una Petición al HSS intermediario 20, usando los detalles recibidos en paso S2, que se recibe en el paso S4 por el HSS intermediario 20.

10 En el paso S5 el HSS intermediario 20 realiza un proceso de selección para determinar cuál del primer y segundo casos de HSS 40 se debería elegir para manejar la Petición; ejemplos de criterios posibles a ser usados en el proceso de selección se exponen más adelante.

15 Habiendo hecho la selección de un caso de HSS 40 adecuado en el paso S5, la AVP del Ordenador Principal de Destino recibida desde el cliente HSS 10 se sustituye en el paso S5a con la AVP del Ordenador Principal de Destino del caso del HSS 40 seleccionado. La Petición entonces se reenvía en el paso S6 mediante el HSS intermediario 20 al caso de HSS 40 seleccionado, el cual se recibe y procesa en el paso S7 por el caso del HSS seleccionado 40.

20 Cuando se ha procesado la Petición, se envía una Respuesta desde el caso de HSS 40 seleccionado al HSS intermediario 20 y se recibe por el HSS intermediario 20 en el paso S9. En el paso S10 la Respuesta se reenvía por el HSS intermediario 20 al cliente del HSS 10, y se recibe por el cliente HSS 10 en el paso S11.

25 Las partes del HSS intermediario 20, la SLF 30 y los casos de HSS 40 para realizar los pasos de la Figura 2 se ilustran esquemáticamente en la Figura 3, con partes P1 y P4 a P10 de la Figura 3 que se adaptan para realizar los pasos S1 y S4 a S10 respectivamente de la Figura 2.

30 Es posible usar un agente intermediario de Diámetro (por ejemplo el HSS intermediario), que interconecta todos los nodos, a nivel de Diámetro. Con esta opción no se necesitan cambios en los nodos cliente actuales, dado que toda la lógica se puede centralizar en el intermediario, el cual sustituye la "AVP del Ordenador Principal de Destino" recibida de los clientes (por ejemplo 10) que direcciona el intermediario 20 con la "AVP del Ordenador Principal de Destino" del caso del HSS seleccionado allí dentro, y que es utilizable para dirigirle un mensaje recibido desde un cliente.

35 Aunque se introduce procesamiento y latencia adicionales por el intermediario, por otra parte las consultas desde los clientes HSS a la SLF se pueden eliminar, y la potencia y retardos de procesamiento que eso implica. Además, los clientes HSS solamente necesitan ser configurados con una dirección del HSS intermediario 20, y no de casos de HSS individuales. Los clientes entonces usan dicha dirección (por ejemplo como la "AVP del Ordenador Principal de Destino" si se usa el protocolo de DIÁMETRO) para enviar mensajes y peticiones que necesitan ser procesadas por un caso de HSS, que hará que estos mensajes y peticiones sean encaminados automáticamente hacia el HSS Intermediario.

40 Es posible duplicar el intermediario. Se pueden usar para esto procedimientos estándar para conmutación por fallo y monitorización de enlace (ver la RFC 3588). La Figura 4 ilustra una arquitectura con múltiples intermediarios de Diámetro 20.

45 Los mensajes de Diámetro que se originan en los clientes HSS tiene el mismo ordenador principal de destino, como si hubiera un único HSS (no SLF) desplegado en la red, que es la dirección del HSS Intermediario 20.

50 El método y el Intermediario de la invención son utilizables, ambos: en arquitecturas monolíticas y de niveles. En resumen, un caso de HSS según una arquitectura monolítica comprende los medios de procesamiento y lógica de aplicaciones, para procesar la señalización a ser intercambiada con los clientes HSS, así como medios de almacenamiento que comprenden los datos necesarios (por ejemplo información dinámica y estática del abonado) para consumir con dicho procesamiento. A su vez, una arquitectura "de niveles" del HSS comprende una pluralidad de circuitos de entrada (FE) de HSS, que comprenden los medios de procesamiento y la lógica de aplicaciones, y una base de datos DB centralizada (física o lógica) que almacena todos los datos necesarios que puede necesitar cualquier FE de HSS para consumir su procesamiento.

55 En el caso de los Circuitos de Entrada del HSS que accede a una Base de Datos (DB) de Abonado, cuando esta DB está distribuida en dos o más emplazamientos, el intermediario puede mantener la información sobre cuál es el Circuito de Entrada (FE) más adecuada o grupo de Circuitos de Entrada, en base a la distribución geográfica de datos, para servir a cada usuario.

60 La aplicación intermediaria de Diámetro mejorada puede monitorizar el estado de los pares de Diámetro que pueden manejar el mensaje para un usuario dado (estos pares podrían ser o bien HSS monolíticos o Circuitos de Entrada con acceso a una base de datos que contiene los datos de usuario). En caso de redundancia, al menos dos pares de Diámetro (por ejemplo los casos de HSS) deberían ser capaces de gestionar cada usuario. El mecanismo usado en los intermediarios de Diámetro para monitorizar los pares de terminación podría ser o bien el mismo incluido en el

estándar de Diámetro (mensajes de Petición de Vigilancia de Dispositivo/Respuesta de Vigilancia de Dispositivo o DWR/DWA; ver la RFC 3588) o bien uno diferente.

5 El intermediario podría distribuir el tráfico entre los diferentes pares de Diámetro que son capaces de manejar la operación, por ejemplo en base a la ubicación geográfica y disponibilidad. Esta distribución se puede basar en un mecanismo de balanceo existente tal como carga del servidor, tiempo de respuesta, rotación equilibrada, etc.

Estos conceptos se ilustran en la Figura 5.

10 Una vez que se ha seleccionado un nodo de terminación adecuado, la AVP del ordenador principal de destino recibida del cliente HSS (es decir la URI de Diámetro de HSS que identifica el HSS lógico único) se sustituye según el par de Diámetro seleccionado, y el mensaje de Diámetro enviado a él.

15 Cuando se recibe una respuesta desde el nodo de terminación, es deseable mantener el ID del ordenador principal de Diámetro consistente (es decir, la respuesta debería llegar desde el Ordenador Principal de Destino usado en la petición). La arquitectura interna de este HSS lógico único es transparente a los clientes del HSS, es decir no se requiere el intermediario para proporcionar al cliente HSS la URI de Diámetro real del ordenador principal de destino seleccionado.

20 Las peticiones desde el HSS también se pueden intermediar. La interfaz intermediaria de Diámetro de HSS permite redundancia en ambas direcciones (la URI de Diámetro del cliente HSS se puede almacenar en el HSS/FE según los procedimientos del estándar del 3GPP).

25 Aunque la presente invención hasta ahora se ha descrito principalmente en relación a un cliente HSS y un HSS, una realización de la presente invención es aplicable de manera más general. En un sentido general, una realización de la presente invención introduce un "agente intermediario de Diámetro" (DPA) (utilizable en, pero no limitado a, una arquitectura de IMS) entre cualquier "cliente de Diámetro" (por ejemplo la Función de Control de Sesión de Llamada CSCF o el Servidor de Aplicaciones AS) y cualquier "ordenador principal de destino" (por ejemplo el HSS).

30 El DPA actúa como un agente intermediario estándar desde el lado del cliente, y está mejorado con respecto al lado del ordenador principal de destino. El DPA puede recibir una petición desde un cliente conteniendo una AVP del "Ordenador Principal de Destino". El DPA traduce la AVP del "Ordenador Principal de Destino" (ficticia) recibida desde un cliente dentro de un identificador utilizable para encaminar la petición hacia el HSS final, que se selecciona por él según la "información de disponibilidad". El DPA de esta manera almacena una tabla que comprende las AVP del "Ordenador Principal de Destino" (ficticio) que se puede recibir desde clientes, que encamina al DPA, y las listas correspondientes de identificadores de las AVP del "Ordenador Principal de Destino" reales de los HSS reales que se pueden seleccionar. La información de disponibilidad por HSS real, que se puede actualizar dinámicamente, así como la información acerca de la ubicación geográfica de los HSS en función de la ubicación de los clientes, también se puede mantener por el DPA y usar para la traducción anterior.

40 Una realización de la presente invención permite redundancia de HSS y/o HLR tanto en escenarios que comprenden una SLF como en escenarios que no comprenden una SLF, y es utilizable para arquitecturas de HSS monolítico o de niveles.

45 El DPA de la invención se puede proporcionar con procedimientos de redundancia de Diámetro estandarizados hacia los clientes, permitiendo por ello el despliegue de una pluralidad de DPA, que proporcionan una disponibilidad elevada de comunicación entre clientes y ordenadores principales de destino. Además, no es necesaria ninguna modificación en los clientes de Diámetro (por ejemplo las CSCF) o los servidores de Diámetro (por ejemplo los HSS), ya que el nuevo procesamiento llevado a cabo por el DPA actúa solamente a nivel de "Diámetro", y no a nivel de aplicaciones (por ejemplo procesamiento relacionado con CX-intf).

50 Se apreciará que la operación de uno o más de los componentes descritos anteriormente se puede controlar mediante un programa que opera en el dispositivo o aparato. Tal programa operativo se puede almacenar en un medio legible por ordenador, o podría, por ejemplo, ser realizado en una señal tal como una señal de datos descargable desde un sitio web de Internet. Las reivindicaciones adjuntas tiene que ser interpretadas como que cubren un programa operativo en sí mismo, o como un registro en una portadora, o como una señal, o en cualquier otra forma.

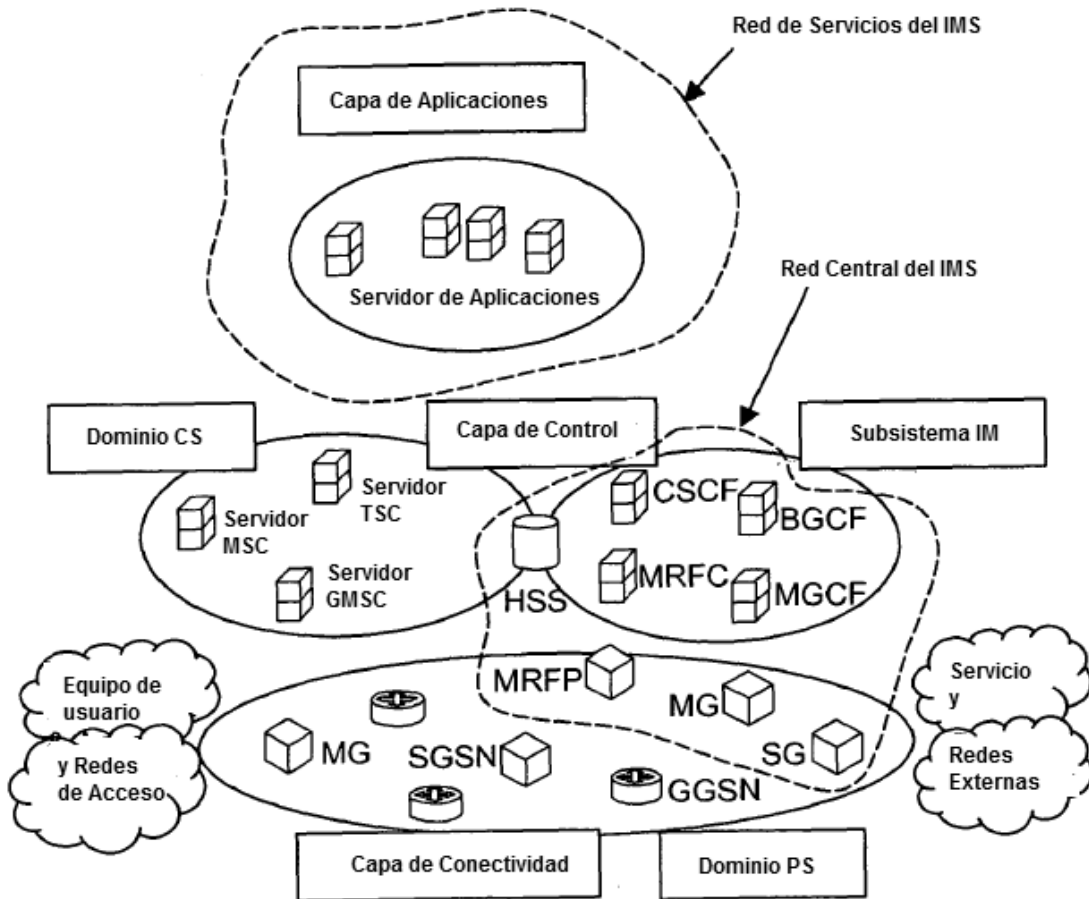
REIVINDICACIONES

- 5 **1.** Un método para permitir redundancia para un Servicio de Abonado Residencial, HSS, de un Subsistema Multimedia IP, IMS, con redundancia que se proporciona por una pluralidad de casos de HSS (40), donde los datos para cada uno de una pluralidad de usuarios se gestiona por más de uno de los casos de HSS, y el método que comprende: donde un nodo cliente (10) del IMS requiera detalles de un HSS, disponer el nodo cliente (10) a ser dotado (S1) con detalles de un HSS intermediario (20) que representa los casos de HSS (40); y disponer el HSS intermediario (20) para: seleccionar (S5) uno adecuado de los casos de HSS (40) para manejar una petición recibida (S4) en el HSS intermediario (20) desde el nodo cliente (10); cambiar (S5a) una Pareja de Valores de Atributos del ordenador principal de destino en la petición recibida en base a la selección; y reenviar (S6) la petición del caso de HSS seleccionado (40) para la manipulación.
- 15 **2.** Un método según la reivindicación 1, que comprende, donde se proporciona una Función de Ubicación de Suscripción (30), SLF, en el IMS, disponer la SLF (30) para dotar al nodo cliente (10) con detalles del HSS intermediario (20).
- 20 **3.** Un método según la reivindicación 1, que comprende, donde no se proporciona una Función de Ubicación de Suscripción (30), SLF, en el IMS, disponer el HSS intermediario (20) en sí mismo para dotar al nodo cliente (10) con detalles del HSS intermediario (20).
- 25 **4.** Un método según la reivindicación 1, 2 o 3, en donde el protocolo Diámetro se usa para comunicación entre el nodo cliente y el HSS intermediario.
- 30 **5.** Un método según cualquier reivindicación precedente, en donde la redundancia del HSS intermediario también se dota, teniendo una pluralidad de casos de HSS intermediario, con redundancia hacia los casos de HSS intermediario que se manejan por mecanismos de protocolo Diámetro estándar.
- 35 **6.** Un método según cualquier reivindicación precedente, en donde al menos algunos de los casos de HSS son diferentes circuitos de entrada respectivos a una base de datos.
- 40 **7.** Un método según cualquier reivindicación precedente, que comprende mantener la información en el HSS intermediario para su uso en la realización de la selección.
- 45 **8.** Un método según la reivindicación 7, en donde la información comprende al menos uno de: información relativa a las cargas respectivas que se experimentan por los casos de HSS; disponibilidades respectivas de los casos de HSS; y estados respectivos de los casos de HSS.
- 50 **9.** Un método según la reivindicación 7 u 8, cuando depende de la reivindicación 6, en donde, donde la base de datos está distribuida a través de una pluralidad de emplazamientos, la información comprende información geográfica relativa a los emplazamientos.
- 55 **10.** Un método según cualquier reivindicación precedente, que comprende monitorizar el estado de cada caso de HSS para su uso en la realización de la selección.
- 60 **11.** Un método según la reivindicación 10, que comprende monitorizar el estado usando mensajes de Diámetro.
- 65 **12.** Un método según la reivindicación 11, que comprende monitorizar el estado usando mensajes de Petición de Vigilancia de Dispositivo/Respuesta de Vigilancia de Dispositivo, DWR/DWA.
- 13.** Un método según cualquier reivindicación precedente, que comprende realizar la selección en base a al menos uno de la ubicación geográfica, la disponibilidad, la carga y el tiempo de respuesta.
- 14.** Un método según cualquier reivindicación precedente, en donde el HSS intermediario es un nodo del IMS y/o en donde el HSS intermediario es un agente intermediario de Diámetro y/o en donde el nodo cliente es un cliente de Diámetro.
- 15.** Un método según cualquier reivindicación precedente, en donde el nodo cliente comprende al menos uno de: una Función de Control de Sesión de Llamada de Interrogación del IMS; una Función de Control de Sesión de Llamada de Servicio del IMS; un Intermediario de Agregación del IMS; y un Servidor de Aplicaciones del IMS.
- 16.** Un aparato para permitir redundancia para un Servicio de Abonado Residencial, HSS, de un Subsistema Multimedia IP, IMS, con redundancia que se proporciona por una pluralidad de casos de HSS (40), donde los datos para cada uno de una pluralidad de usuarios se gestionan por más de uno de los casos de HSS (40), y el aparato que comprende: medios (P1) para disponer, donde un nodo cliente (10) del IMS requiera detalles de un HSS, el nodo cliente (10) para ser dotado con detalles de un HSS intermediario (20) que representa los casos de HSS (40); y

medios (P5, S5a, P6) para disponer el HSS intermediario (20) para: seleccionar uno adecuado de los casos de HSS (40) para manejar una petición recibida en el HSS intermediario (20) desde el nodo cliente (10); cambiar una Pareja de Valores de Atributos del ordenador principal de destino en la petición recibida en base a la selección; y reenviar la petición del caso de HSS seleccionado para la manipulación.

- 5
- 17.** Un aparato según la reivindicación 16, en donde el aparato comprende el HSS intermediario.
- 18.** Un programa para controlar un aparato para realizar los pasos del método del HSS intermediario de cualquiera de las reivindicaciones 1 a 15.
- 10
- 19.** Un medio de almacenamiento que contiene un programa según la reivindicación 18.

FIG. 1



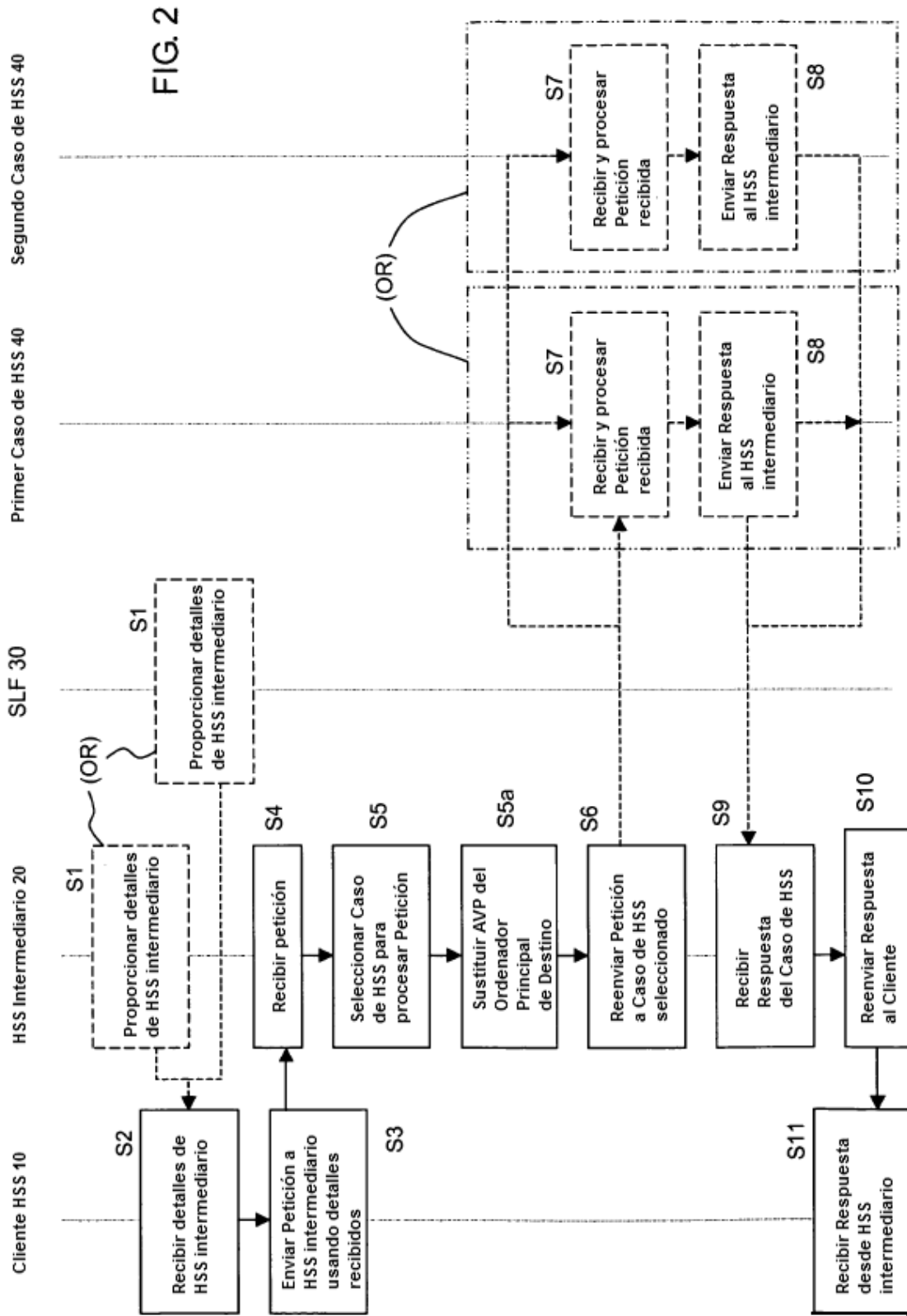
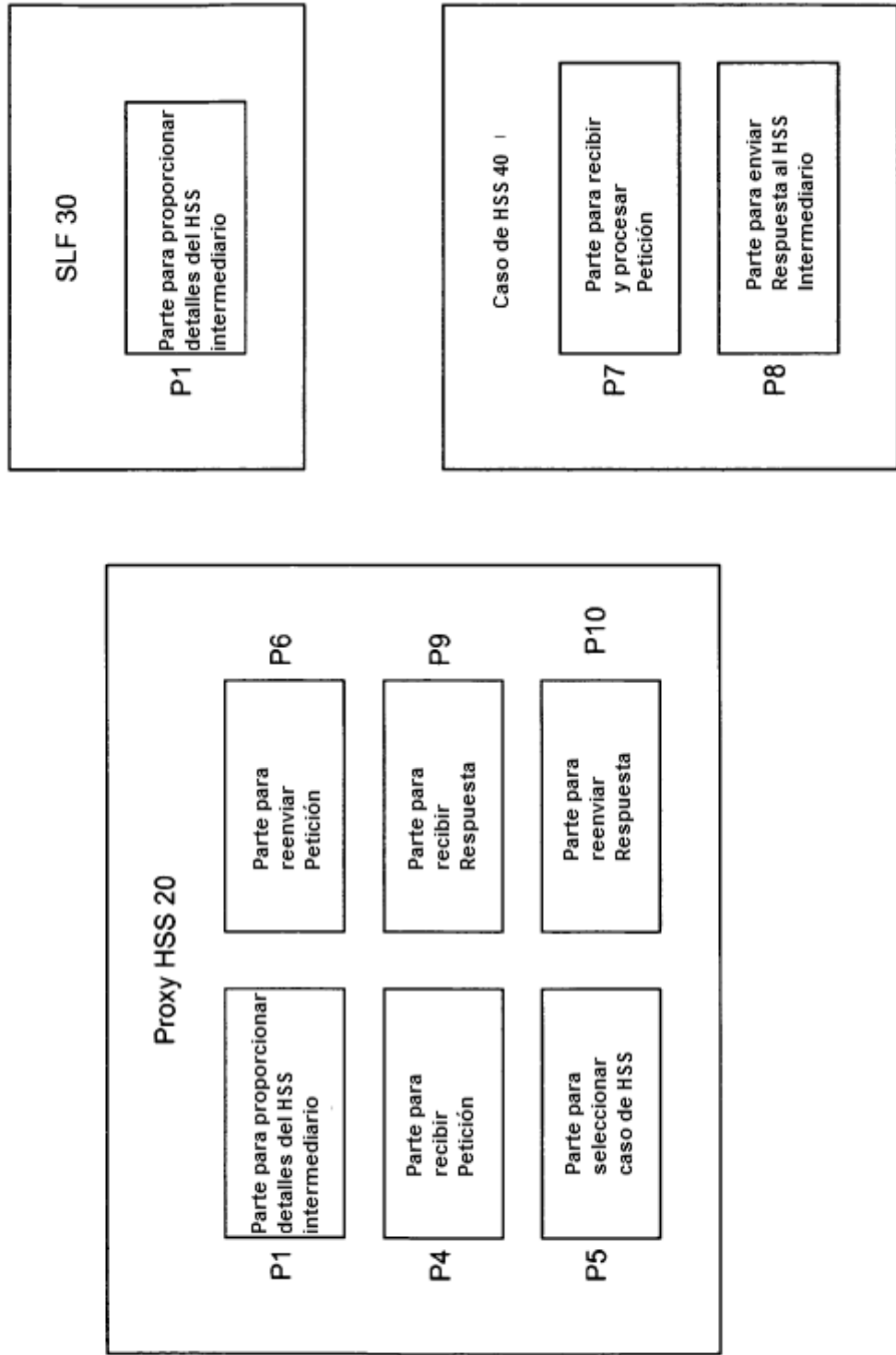


FIG. 3



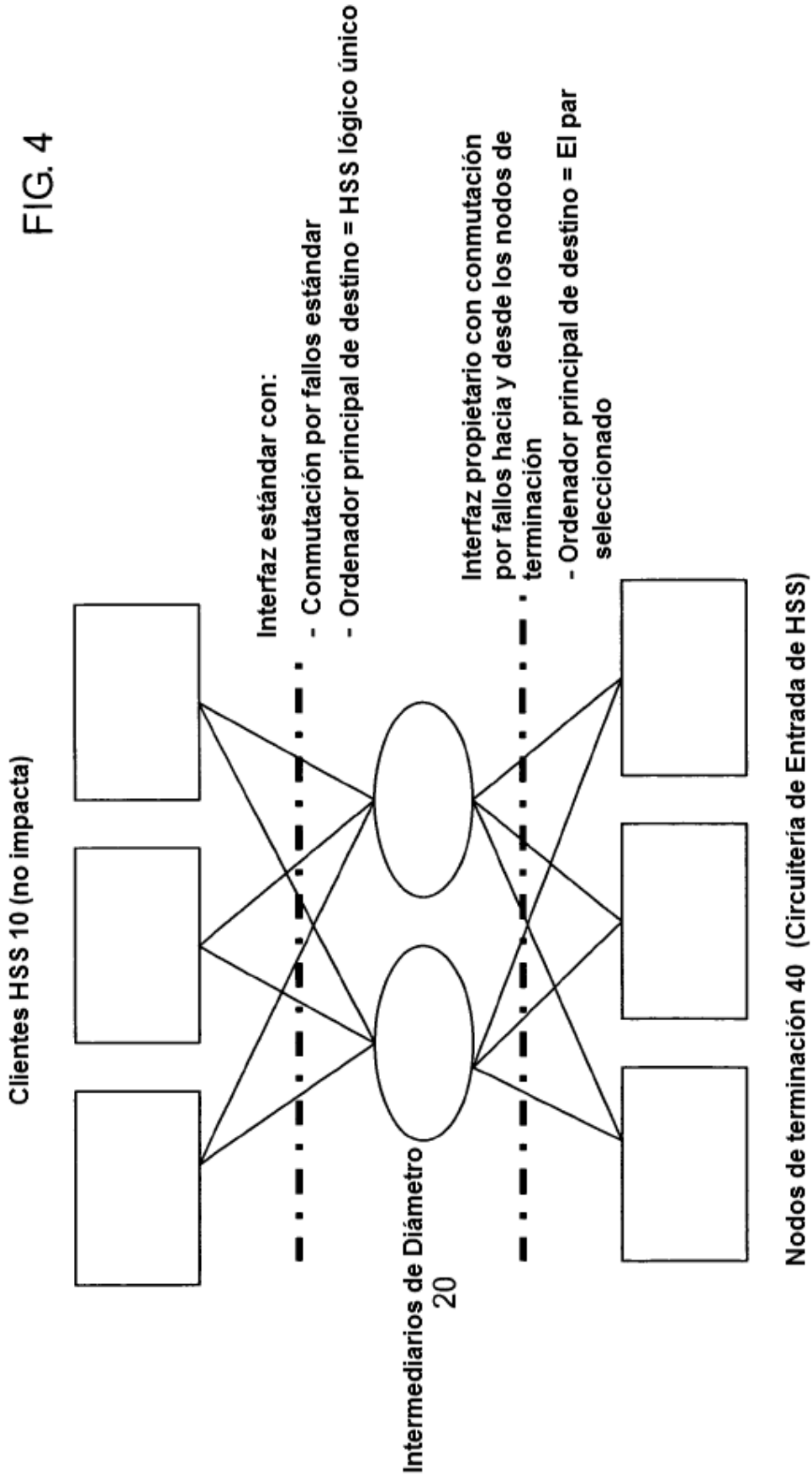


FIG. 5

