(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 564 423**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.12.2005 E 05820039 (5)**

(97) Fecha y número de publicación de la concesión europea: **16.12.2015 EP 1964349**

(54) Título: **Técnica para proporcionar interoperabilidad entre diferentes dominios de protocolo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.03.2016

(73) Titular/es:

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

(72) Inventor/es:

LEVENSHTEYN, ROMAN y
FIKOURAS, IOANNIS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Técnica para proporcionar interoperabilidad entre diferentes dominios de protocolo

Campo de la Invención

La invención se refiere a una técnica para proporcionar interoperabilidad entre diferentes dominios de protocolo. La técnica se adapta particularmente para uso en conexión con el dominio de subsistema multimedia de protocolo de Internet (IMS). A este respecto, la presente invención se diseña para proporcionar interoperabilidad con un protocolo de control de sesión IMS.

Antecedentes de la Invención

El IMS es una arquitectura de red de próxima generación (NGN) estandarizada para operadores de red que proporciona servicios multimedia móviles y fijos. Usa una implementación estandarizada del Proyecto de Cooperación de 3ª Generación (3GPP) de SIP y se ejecuta sobre el protocolo de Internet (IP) estándar. También se soportan los sistemas telefónicos existentes (tanto de paquetes conmutados como de circuitos conmutados). IMS usa protocolos IP estándar abiertos como se define por el Grupo de Trabajo de Ingeniería de Internet (IETF). De este modo, se puede establecer una sesión multimedia por ejemplo entre dos usuarios IMS, entre un usuario IMS y un usuario en Internet o entre dos usuarios en Internet usando exactamente los mismos protocolos. IMS funde los mundos de Internet y celular usando tecnologías celulares para proporcionar acceso ubicuo y tecnologías de Internet para proporcionar servicios atractivos.

El IMS comprende tres componentes principales: la función de control de sesión de llamada de servicio (S-CSCF) en una capa de control y el servidor local de abonado (HSS) así como un servidor de aplicaciones (AS) del protocolo de inicio de sesiones (SIP) en una capa de aplicaciones.

El protocolo SIP es una tecnología de control central de IMS. Se usa para controlar sesiones multimedia combinando por ejemplo flujos de voz y datos. Esencialmente, SIP es un protocolo basado en texto para sesiones de comunicación entre las partes. En particular, SIP se usa para el establecimiento, control y finalización de sesiones de comunicación entre aplicaciones basadas en red y también para el control de canales de medios entre esas aplicaciones. Después de que se establece una sesión, se pueden usar otros protocolos para comunicación entre aplicaciones. De esta manera, las funciones principales de SIP son control de sesión, direccionamiento y gestión de movilidad en el nivel de servicio.

IMS proporciona un montón de funciones comunes usadas por redes móviles, tales como AAA (autenticación, autorización y contabilidad), tarificación, control de acceso y HSS (es decir, bases de datos de perfil de usuario). Estas funciones de IMS se entienden que se usan por aplicaciones convergentes de una forma uniforme, de manera que no hay necesidad de tener mecanismos separados aplicados por ejemplo a comunicaciones de voz y de datos.

En paralelo al dominio IMS, se ha desarrollado el concepto de Servicios Web (WS) de Lenguaje de Marcas Extensible (XML). WS de XML son una tecnología relativamente nueva para la creación de sistemas distribuidos, altamente interoperables. WS de XML se basan en estándares basados en XML, como Protocolo de Acceso de Objetos Simple (SOAP), Lenguaje de Definición de Servicios Web (WSDL) y Descripción, Descubrimiento e Integración Universal (UDDI). Los Servicios Web son una plataforma transversal interoperable e independiente del lenguaje de programación. Han llegado a ser un medio popular de desarrollo e integración de sistemas de sistemas de empresa y aplicaciones de red. Debido a su flexibilidad y un diseño que está más alineado con redes IT, las arquitecturas basadas en Servicios Web, por ejemplo, Arquitecturas Orientadas a Servicios (SOA), están emergiendo rápidamente y es probable que sean adoptadas en diseño de red de comunicación móvil.

La mayoría de Servicios Web no tienen estado, lo cual significa que cada invocación del Servicio Web debería contener toda la información que necesita procesar una solicitud, dado que el procesamiento depende solamente de estos datos. Este diseño simplifica extremadamente la implementación de WS. Recientemente, no obstante, muchos investigadores y profesionales en el área de WS se han dado cuenta de que también hay una necesidad de Servicios Web con estado. Tales servicios con estado son particularmente importantes para transacciones que implican varias invocaciones de servicio. Son igualmente importantes donde se requiera una correlación entre mensajes, por ejemplo, banca electrónica y reserva de billetes. Varias especificaciones de WS que abordan estos asuntos, por ejemplo, Contexto de WS, Direccionamiento de WS y Estructura de Recursos de WS, se han presentado a estandarización, pero la mayoría de éstas simplemente complementan cabeceras de SOAP de WS a través de cabeceras de información de sesión.

La arquitectura de IMS define que todas las invocaciones de servicio entrantes sean llevadas a cabo sobre sesiones SIP. Los nodos de IMS, por ejemplo, CSCF-I y la CSCF-P, son servidores SIP que manejan mensajes SIP entrantes. No obstante, incluso hoy en día existen muchos servicios basados en no SIP en el dominio de operador y estos servicios a menudo usan protocolos y tecnologías no SIP (por ejemplo, Servicios Web, pero también J2EE, .NET, etc.).

Proporcionar acceso para usuarios externos a servicios, en particular servicios no SIP, en el dominio IMS no es posible generalmente debido a que las aplicaciones de consumidor de servicio no SIP de terceras partes externas típicamente no son conscientes del hecho de que el servicio invocado está situado dentro del dominio IMS y tales aplicaciones de consumidor externas típicamente no soportan SIP. Por lo tanto, un consumidor de servicio no SIP es incapaz de acceder al servicio en cuestión dentro del dominio IMS, lo que reduce extremadamente la disponibilidad y por lo tanto el valor del servicio.

SIP y WS abordan problemas similares, pero cada uno tiene sus propias soluciones para gestión de sesión. En otras palabras, los planteamientos usados para gestión de sesión por SIP y WS son independientes uno de otro. Como resultado, los Servicios Web desplegados dentro del dominio IMS requieren su propia infraestructura de WS incompatible con IMS, incluyendo autenticación, contabilidad, tarificación y otra funcionalidad IMS. Además, las invocaciones de WS se ejecutan en base a URL (localizadores de recursos únicos) que requieren un conocimiento preciso de la dirección de red actual del servicio (por ejemplo, el número de IP, nombre de DNS, etc.). Esto significa que los usuarios no pueden invocar servicios alojados en plataformas móviles (por ejemplo, terminales móviles y nodos de red que cambian regularmente su URL) hasta que se conoce su URL actual.

No obstante, las cabeceras de invocación SOAP de Servicios Web se complementan a través de cabeceras de información de sesión. Esto puede conducir a mensajes SOAP grandes comparados con el tamaño de la carga útil. Tales cabeceras se envían con cada mensaje SOAP y de esta manera consumen más ancho de banda que los Servicios Web sin sesión. El aumento de tráfico puede ser un problema especial en los entornos móviles por el aire, donde podría introducir una carga de red mayor y conducir a latencias mayores. Aunque se pueden emplear esquemas de compresión para comprimir y descomprimir mensajes SOAP para abordar este problema, estos se han mostrado que son muy intensivos en recursos y consumen tiempo, incluso con terminales móviles de alta gama.

Por consiguiente, hay una necesidad de una técnica para proporcionar un aumento de interoperabilidad entre servicios situados dentro del dominio IMS y componentes de cliente situados fuera del dominio IMS.

La publicación del IEEE titulada “THE IMS PLAYGROUND @ FOKUS – AN OPEN TESTBED FOR NEXT GENERATION NETWORK MULTIMEDIA SERVICES” de Magedanz, T. et al., introduce el estándar IMS y proporciona una visión general del Campo de juego de IMS Abierto a FOKUS. Otro documento titulado “The Convergence of Circuit and Packet Core Networks” de Ejzak et al., describe una arquitectura que unifica los dominios de circuito e IMS proporcionando un único plano de control para ambos.

Sumario de la Invención

Según un aspecto, la presente invención proporciona un método según la reivindicación del método independiente 1 de provisión de interoperabilidad entre un dominio de subsistema multimedia de protocolo Internet (IMS) y un dominio no IMS. El método comprende, entre otros, los pasos de recibir en una capa de servicio un mensaje de invocación de servicio desde un dominio no IMS, analizando el mensaje para identificar el mensaje como una solicitud para invocar un servicio dentro del dominio IMS, convirtiendo en una capa de control de sesión elementos de protocolo de control de sesión no IMS relacionados con el mensaje en elementos de protocolo relacionados con control de sesión IMS y enviando uno o más mensajes hacia el dominio IMS para proporcionar una sesión de control IMS en el dominio IMS en base a los elementos de protocolo relacionados con control de sesión IMS.

En un ejemplo, el paso de conversión se puede basar en un esquema de correspondencia que asocia elementos de protocolo de control de sesión no IMS individuales con elementos de protocolo relacionados con control de sesión IMS individuales. Los elementos de protocolo incluyen tipos de mensajes específicos de protocolo (tales como mensajes de invocación de servicio), partes de mensajes (tales como cabeceras) y campos de mensaje (tales como campos de cabecera que especifican direcciones particulares).

El método también puede incluir el paso de reenviar en la capa de servicio el mensaje de invocación de servicio usando la sesión de control IMS. El método además puede incluir los pasos de recibir al menos un mensaje adicional desde el dominio no IMS relacionado con el servicio invocado dentro del dominio IMS y reenviar en la capa de servicio el mensaje de servicio usando la sesión de control IMS. También se puede usar aquí un esquema de correspondencia para asociar un solicitante de servicio particular (por ejemplo, una aplicación o un componente de red fuera del dominio IMS) con una o más sesiones solicitadas (y/o en marcha) dentro del dominio IMS.

El método de la invención puede incluir además los pasos de recibir un mensaje desde el dominio IMS durante la sesión, convirtiendo los elementos de protocolo relacionados con control de sesión IMS relacionados con el mensaje del dominio IMS en elementos de protocolo de control de sesión no IMS, generando un mensaje no IMS en base a los elementos de protocolo de control de sesión no IMS y enviando el mensaje no IMS durante la sesión hacia el dominio no IMS.

En una variante de la invención, el servicio dentro del dominio IMS es un servicio basado en protocolo IMS. Por ejemplo, el servicio en el dominio IMS podría ser una función de soporte de IMS que puede incluir una o más de las siguientes funciones: autenticación, autorización, contabilidad (por ejemplo, AAA), tarificación, control de acceso y HSS. Aquí, el protocolo de control de sesión IMS puede ser el protocolo DIAMETER que proporciona por ejemplo

información de contabilidad para el servicio. El servicio en sí mismo se puede proporcionar desde dentro o desde fuera del dominio IMS.

En otra variante, el servicio en el dominio IMS es una aplicación basada en protocolo no IMS (por ejemplo, un servicio accesible mediante programación tal como una aplicación basada en Servicios Web operada desde dentro del dominio IMS). Aquí, el protocolo de control de sesión IMS puede ser SIP que controla la provisión (por ejemplo, establecimiento y/o gestión general) de la sesión de servicio IMS.

Los elementos de protocolo de control de sesión no IMS preferiblemente comprenden cabeceras de un protocolo de control de sesión no IMS y los elementos de protocolo relacionados con control de sesión IMS preferiblemente comprende cabeceras tales como cabeceras SIP. A modo de ejemplo, el servicio basado en protocolo no IMS puede emplear un protocolo de mensajería basado en Lenguaje de Marcas (ML), tal como Servicios Web de XML.

El método además incluye los pasos de analizar el mensaje recibido desde el dominio no IMS y/o desde el dominio IMS, determinando un estado de la sesión con el servicio en el dominio IMS en base al mensaje analizado y almacenar el estado de la sesión. Almacenar el estado de una sesión particular facilita la correspondencia entre servicios individuales dentro del dominio IMS y las sesiones individuales (que se extienden potencialmente en el dominio no IMS).

Según un aspecto adicional, se puede comprobar (por ejemplo, en respuesta a la recepción de un mensaje desde el dominio no IMS) si está en marcha una sesión con un servicio en el dominio IMS y, si no hay ninguna sesión en marcha, se puede establecer una nueva sesión bajo un protocolo de control de sesión IMS tal como SIP. Preferiblemente, los mensajes no IMS se autentican anterior a establecer la sesión de control en el dominio IMS. La autenticación se puede realizar analizando una dirección especificada en un mensaje no IMS.

En una variante, el método incluye además los pasos de emplear un esquema de direccionamiento uniforme usando direccionamiento SIP para la invocación de servicios fijos y/o móviles. De este modo, cuando el servicio a ser invocado reside en una plataforma móvil dentro del dominio IMS, el método además puede comprender el paso de definir un identificador de recursos único (URI) de SIP para invocación dinámica del servicio en el dominio IMS, con independencia de un localizador de recursos único (URL) actual para la plataforma móvil.

De esta manera, un concepto adicional que puede operar independientemente de la conversión de elementos de protocolo descrita anteriormente es un método de direccionamiento e invocación de servicios fijos y móviles que usa un esquema de direccionamiento uniforme por medio de direccionamiento SIP, que comprende los pasos de definir el uso de un URI de SIP para invocación dinámica de servicios móviles con independencia de su URL actual (por ejemplo, definiendo una extensión para Direccionamiento de WS) y/o definiendo el direccionamiento fijo de servicios usando un URL de SIP. En lugar de SIP, se podrían usar también otros protocolos de control de sesión IMS para propósitos de direccionamiento e identificación.

Según otro aspecto, la presente invención proporciona un producto de programa de ordenador que comprende partes de código de programa para realizar los pasos del método cuando el producto de programa de ordenador se ejecuta en uno o más ordenadores o sistemas informáticos. El producto de programa de ordenador se puede almacenar en un medio de grabación legible por ordenador.

Según un aspecto adicional, la presente invención proporciona un procesador de ordenador y una memoria acoplada al procesador, en donde la memoria se codifica con uno o más programas que pueden realizar pasos para proporcionar interoperabilidad entre un dominio IMS y un dominio no IMS según el método de la invención descrito anteriormente.

Aún según un aspecto adicional de la invención, se proporciona un dispositivo de correspondencia según la reivindicación del aparato independiente adjunta a la misma para proporcionar interoperabilidad entre un dominio de subsistema multimedia de protocolo de Internet (IMS) y un dominio no IMS. El dispositivo de correspondencia comprende, entre otras cosas, una unidad de análisis para analizar mensajes de invocación de servicio entrantes recibidos en una capa de servicio desde el dominio no IMS, para identificar si uno de los mensajes de invocación de servicio es una invocación de un servicio dentro del dominio IMS, una unidad de conversión para convertir en una capa de control de sesión elementos de protocolo de control de sesión no IMS relacionados con uno de los mensajes en los elementos de protocolo relacionados con control de sesión IMS y una unidad de mensajería para generar uno o más mensajes para proporcionar una sesión de control IMS en el dominio IMS en base a los elementos de protocolo relacionados con control de sesión IMS.

El dispositivo de correspondencia de la invención se puede implementar como una pasarela entre el dominio IMS y el dominio no IMS. Alternativamente, el dispositivo de correspondencia se puede integrar en una pila de protocolo de un componente de red en el dominio no IMS. También se pueden usar otras implementaciones.

Breve descripción de los dibujos

Las realizaciones particulares de la presente invención se describirán ahora con referencia a los dibujos anexos, en los que números de referencia iguales identifican rasgos iguales y en los cuales:

la Figura 1 es un diagrama de flujo esquemático que ilustra una realización del método según la presente invención;
la Figura 2 es una ilustración esquemática de una realización del dispositivo de correspondencia según la presente invención que opera para convertir mensajes recibidos desde el dominio no IMS;
la Figura 3 es una ilustración esquemática de una realización del dispositivo de correspondencia según la presente invención que opera para convertir mensajes recibidos desde el dominio IMS;
la Figura 4 ilustra una realización según la presente invención incorporada como una pasarela SOAP sobre SIP para acceder a Servicios Web en el dominio IMS;
la Figura 5 ilustra una realización según la presente invención incorporada como un tiempo de diseño de correspondencia de sesión SOAP a SIP para acceder a Servicios Web en el dominio IMS;
la Figura 6 ilustra una realización según la presente invención incorporada como una correspondencia SOAP sobre SIP para acceder transparentemente a facilidades IMS para gestión de usuario/servicio; y
la Figura 7 ilustra una realización según la invención que usa URI de SIP para implementar direccionamiento de servicios móviles.

Descripción detallada de la Invención

En la siguiente descripción, con propósitos de explicación y no de limitación, se exponen detalles específicos, tales como secuencias de pasos particulares, estándares de protocolo y diversas configuraciones de dispositivos a fin de proporcionar una comprensión minuciosa de la presente invención. Se entenderá que la presente invención se puede poner en práctica en otras realizaciones que se apartan de estos detalles específicos.

Además, los expertos en la técnica apreciarán que las funciones explicadas en la presente memoria más adelante se pueden implementar usando software que funciona en conjunto con un microprocesador u ordenador de propósito general programado y/o usando un circuito integrado de aplicaciones específicas (ASIC).

La técnica para proporcionar interoperabilidad entre diferentes dominios de protocolo según la presente invención se describirá en primer lugar con referencia a las Figuras 1 y 2. La Figura 1 ilustra esquemáticamente una realización del método para proporcionar interoperabilidad entre un dominio IMS y un dominio no IMS. De la misma manera, la Figura 2 ilustra esquemáticamente una realización de un dispositivo de correspondencia 100, que opera para proporcionar esta interoperabilidad entre el dominio IMS y el dominio no IMS.

Con referencia a ambas de las Figura 1 y 2, el primer paso S1 del método implica recibir en una capa de servicio (o aplicación) un mensaje de invocación de servicio 101 desde el dominio no IMS. Este mensaje 101 se recibe por el dispositivo de correspondencia 100. El segundo paso S2 del método implica analizar el mensaje recibido desde el dominio no IMS. En otras palabras, el mensaje 101 recibido por el dispositivo de correspondencia 100 se somete a análisis en una unidad de análisis 102 del dispositivo de correspondencia. El tercer paso S3 implica identificar el mensaje de invocación de servicio recibido desde el dominio no IMS como una solicitud para invocar un servicio dentro del dominio IMS (comparado, por ejemplo, con un servicio que va a ser proporcionado desde fuera del dominio IMS). Este servicio puede ser, por ejemplo, una función de soporte IMS, tal como AAA o HSS o un servicio no IMS proporcionado desde dentro del dominio IMS. El paso de identificar la naturaleza del mensaje 101 recibido por el dispositivo de correspondencia 100 se lleva a cabo típicamente por la unidad de análisis 102.

Después de que el mensaje 101 recibido desde el dominio no IMS se ha identificado como una invocación de un servicio dentro del dominio IMS, el método incluye el paso adicional S4 de conversión de elementos de protocolo de control de sesión no IMS relacionados con el mensaje de invocación de servicio en elementos de protocolo relacionados con control de sesión IMS. A este respecto, el método de la invención proporciona una conversión o correspondencia de, por ejemplo, cabeceras de protocolo de control de sesión no IMS en cabeceras de protocolo de un protocolo de control de sesión IMS, tal como SIP. Para este fin, el dispositivo de correspondencia 100 incluye una unidad de conversión 104 para emprender esta conversión de elementos de protocolo no IMS en elementos de protocolo IMS.

La conversión se puede soportar a través de información contenida en campos de mensajes de invocación entrantes. Tal información se puede recopilar desde: la dirección IP del remitente, posiblemente también su dirección DNS, campos específicos de servicio tales como los mensajes de Servicios Web (por ejemplo, SOAP, Contexto de WS) e información de autenticación en forma de credenciales incluidas en el mensaje.

Por ejemplo en el caso de CORBA, los campos de request_id y service_contexts se pueden usar para derivar información relacionada con la transacción o sesión, mientras que campos tales como requesting_principal y operation se pueden usar para derivar información relacionada con los campos Desde y A de SIP. En general este tipo de información se puede convertir por una correspondencia a campos de establecimiento de sesión SIP tales como Desde, A, Permitir, Soportado y Contacto.

El método entonces incluye el paso adicional S5 de generación de un mensaje saliente 107 en contexto con proporcionar una sesión de control IMS (por ejemplo, establecer una sesión de control o controlar una sesión de control establecida) en el dominio IMS en base a los elementos de protocolo relacionados con control de sesión IMS. El establecimiento de la sesión puede implicar el intercambio de varios mensajes entre el dispositivo de correspondencia 100 y el servicio. Por consiguiente, el dispositivo de correspondencia puede asumir el papel de un socio de comunicación durante el establecimiento de sesión en el dominio IMS.

Naturalmente, además de, por ejemplo, un mensaje inicial desde el dominio no IMS invocando el servicio dentro del dominio IMS, se pueden recibir adicionalmente uno o más mensajes adicionales 101 desde el dominio no IMS. A este respecto, la unidad de mensajería 106 del dispositivo de correspondencia 100 está adaptada para generar un mensaje IMS saliente correspondiente para controlar la sesión una vez que se ha establecido.

De manera similar, con referencia ahora a la Figura 3, también puede ser el caso de que se reciba un mensaje 107 desde el dominio IMS durante la sesión que se ha establecido para el servicio invocado. Un mensaje 107 recibido desde el dominio IMS se maneja por el dispositivo de correspondencia 100 de una manera recíproca. Específicamente, los elementos de protocolo relacionados con control de sesión IMS, tales como cabeceras SIP, contenidas en ese mensaje se pueden convertir por la unidad de conversión 104 en elementos de protocolo de control de sesión no IMS y se puede generar un mensaje no IMS correspondiente por la unidad de mensajería 106. El dispositivo de correspondencia 100 entonces envía este mensaje no IMS 101 al dominio no IMS en el curso de la sesión establecida o a partir de entonces. Se apreciará que, en las Figura 2 y 3, el número de referencia 101 identifica un mensaje no IMS y el número de referencia 107 identifica uno IMS.

Las siguientes realizaciones proporcionan planteamientos genéricos para permitir interoperabilidad entre servicios no SIP y SIP orientados a sesión. Además, las realizaciones también permiten la provisión de funcionalidad de sesión a tecnologías de servicio no orientadas a sesión (por ejemplo, Servicios Web).

La correspondencia entre servicios no SIP y sesiones SIP se consigue por una entidad (por ejemplo, el dispositivo de correspondencia 100 mostrado en las Figura 2 y 3 o un dispositivo diferente) que almacena el estado de la sesión particular analizando sintácticamente mensajes entrantes (posiblemente en un número de diferentes protocolos). Este conocimiento se usa entonces para generar mensajes salientes adecuados (de nuevo posiblemente en un número de diferentes protocolos posibles).

Las aplicaciones no SIP (desde fuera el dominio IMS) que son servicios no basados en sesión e invocados desplegados dentro del dominio IMS no son conscientes de SIP y, por lo tanto, no son capaces de establecer y mantener sesiones como se requiere por IMS. Por esta razón, la implementación del dispositivo de correspondencia de sesión se ocupa de la iniciación y gestión de sesiones para las aplicaciones en cuestión, como se requiere por la parte consciente de sesión de la transacción. Esto puede requerir que todos los mensajes entre el servicio invocador y el invocado sean encaminados a través del dispositivo de correspondencia.

Para lograr esto, el operador puede encaminar todo el tráfico entrante relacionado con servicios IMS disponibles públicamente a través del dispositivo de correspondencia (por ejemplo, en IP o niveles más altos). Por ejemplo, los servicios en el dominio IMS se podrían exponer a través de un URL o cualquier otro mecanismo de direccionamiento alojado en el dispositivo de correspondencia. El operador puede publicar este URL a partes externas para propósitos de direccionamiento.

Por el bien de la claridad, las realizaciones usadas para ilustrar el planteamiento técnico suponen que el servidor de aplicaciones que aloja servicios no SIP ejemplares dentro del dominio IMS contiene tanto pilas SIP como no SIP (por ejemplo, WS, J2EE, CORBA, etc.) adecuadas al servicio que se invoca. Incluso aunque otras configuraciones posibles puedan implicar diferentes pilas de protocolo desplegadas en diferentes configuraciones de nodos, el planteamiento técnico general sigue siendo el mismo.

A continuación, se describirá una realización de un mecanismo de correspondencia de sesión con referencia a una aplicación no SIP A (que se ejecuta por ejemplo sobre un terminal de usuario capaz de WS situado fuera del dominio IMS) que invoca un servicio B dentro del dominio IMS. La aplicación no SIP actúa de esta manera como un cliente con respecto al servicio IMS B.

La correspondencia de sesión se puede conseguir con los siguientes pasos:

1. Las solicitudes entrantes desde aplicaciones no SIP se pueden autenticar en base a un número de mecanismos que se describen más adelante en más detalle.
2. En base a la autenticación de la aplicación no SIP A que invoca el servicio IMS B, el dispositivo de correspondencia 100 comprueba si ya tiene conocimiento de una transacción de capa de servicio en marcha (que corresponde a una sesión particular en la capa de control de sesión en el dominio IMS) entre la aplicación no SIP A y el servicio IMS B. Para este fin, se puede consultar una tabla de correspondencia que puede enumerar una pluralidad de sesiones establecidas previamente para la aplicación no SIP A y/o cualquier otra aplicación no SIP A'.

3. Si no hay ninguna transacción en marcha entre la aplicación no SIP A y el servicio IMS B, se inicializa una nueva sesión SIP. Aquí, el dispositivo de correspondencia 100 juega el papel del socio de comunicación en la sesión SIP establecida con el servicio IMS B.

a. En caso de que la aplicación no SIP A no sea consciente de la sesión, el dispositivo 100 establece una nueva sesión sin tener en consideración adicional las capacidades de la aplicación no SIP A.
b. En caso de que la aplicación no SIP A sea consciente de la sesión, el dispositivo 100 establecerá la nueva sesión según las capacidades de sesión de la aplicación no SIP A (por ejemplo, Contexto de WS, Direccionamiento de WS, Cabeceras, etc.). El primer ejemplo siguiente ilustra la invocación de servicio creada por el cliente de WS A usando la especificación de Contexto de WS para gestión de sesión de WS. El segundo ejemplo ilustra cómo el dispositivo de correspondencia 100 establece una nueva sesión SIP con el servicio IMS B, usando la información de sesión recopilada a partir de la correspondencia del mensaje SOAP interceptado por el dispositivo de correspondencia 100. Esta configuración implica que el servicio B contiene tanto pilas SIP como WS. Otras configuraciones posibles podrían implicar diferentes pilas de protocolo desplegadas en diferentes nodos.

Un ejemplo de un mensaje de invocación de servicio basado en XML que especifica una sesión de Contexto de WS se da más adelante:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2002/06/soap-envelope">
  <soap:Header>
    <context xmlns="http://docs.oasis-open.org/wscaf/2004/09/wsctx" timeout="100"
      xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
      xmlns:soapbind=http://schemas.xmlsoap.org/wsdl/soap/
      soap:mustUnderstand="1">
      <context-identifier>
        http://services.operator.com/wscaf/2004/09/wsctx/abcdef:012345
      </context-identifier>
      <type>
        http://services.operator.com/wscaf/2004/09/wsctx/context/mmservice
      </type>
    </context>
  </soap:Header>
  <soap:Body>
    <!-- Application Payload -->
  </soap:Body>
</soap:Envelope>
```

El dispositivo de correspondencia 100 convierte los elementos no SIP incluidos en el mensaje de invocación de servicio anterior en un mensaje de establecimiento de sesión SIP que especifica la información de sesión a partir de la sesión de Contexto de WS como sigue:

```
INVITE sips:service1@operator.com SIP/2.0
Via: SIP/2.0/TLS server.operator.com:5061;branch=z9hG4bK74bf9
Max-Forwards: 70
From: SESSION1 <sips:sipsoapgw@operator.com>;tag=1234567
To: SIPAS <sips:service1@operator.com>
Call-ID: 12345601@operator.com
```

```
CSeq: 1 INVITE
Contact: <sips:sipsoapgw@operator.com>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces
Content-Type: application/sdp
Content-Length: ...
v=0
o=servicebroker 2890844526 2890842807 IN IP4 asb.operator.com
s=Conference Service
t=0 0
m=audio 5004 RTP/AVP 0
c=IN IP4 131.160.1.112
a=rtpmap:0 PCMU/8000
m=message 49172 IMTP/TCP application/soap+xml
c=IN IP4 asb.operator.com
a=direction:both
a=wsdl:http://schemas.operator.com/conferencecontrol.wsdl
a=wscafcontextidentifier:http://services.operator.com/wscaf/2004/09/wsctx/abcdef:012345
a=wscaftype:http://services.operator.com/wscaf/2004/09/wsctx/context/mmservice
```

4. En el caso de una transacción existente, su estado se actualiza en base al(a los) mensaje(s) procesados.
5. Los elementos SOAP usados para transportar información de sesión se convierten a cabeceras SIP y viceversa.

Las transacciones ya asignadas a sesiones SIP pueden evitar volver a enviar información relacionada con la sesión de WS en los mensajes SOAP que ya se negoció durante el inicio de sesión SIP. Los ejemplos siguientes ilustran cómo en base a una sesión SIP establecida (como se describió en el paso 3b) la información relacionada con la sesión de Contexto de WS para invocación de servicio WS se puede optimizar a través de evitar la repetición de la información relacionada con el Contexto de WS en la cabecera SOAP.

a) Un ejemplo de invocación de servicio que especifica una sesión de Contexto de WS:

```
<soap:Envelope
xmlns:soap="http://www.w3.org/2002/06/soap-envelope">
  <soap:Header>
    <context xmlns="http://docs.oasis-open.org/wscaf/2004/09/wsctx" timeout="100"
      xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
      xmlns:soapbind=http://schemas.xmlsoap.org/wsdl/soap/
      soap:mustUnderstand="1">
      <context-identifier>
        http://services.operator.com/wscaf/2004/09/wsctx/abcdef:012345
      </context-identifier>
      <type>
        http://services.operator.com/wscaf/2004/09/wsctx/context/mmservice
      </type>
    </context>
  </soap:Header>
```

```
<soap:Body>
  <!-- Application Payload
    MMService specific payload -->
</soap:Body>
</soap:Envelope>
```

b) Un ejemplo de invocación de servicio optimizada sin especificación explícita de una sesión de Contexto de WS:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2002/06/soap-envelope">
  <soap:Header>
  </soap:Header>
  <soap:Body>
    <!-- Application Payload
      MMService specific payload -->
  </soap:Body>
</soap:Envelope>
```

6. Los mensajes SIP generados de esta manera se reenvían al servicio IMS B.

Antes de que se pueda aplicar una autenticación basada en un sobre SOAP como se describe en el paso 3 del algoritmo anterior, ha de ser alcanzado un acuerdo entre el consumidor del servicio y el proveedor de servicios sobre cómo proporcionar las credenciales requeridas. Tales credenciales se pueden intercambiar usando el siguiente protocolo:

1. El operador, como proveedor de servicios, define un formato para el intercambio de credenciales incluyendo diversos tipos de datos que describen la aplicación y que autentican al usuario (por ejemplo, nombre de inicio de sesión, contraseña, nombre de aplicación, etc.). Tal formato se puede implementar por varios medios, por ejemplo, extendiendo la descripción WSDL del servicio dado para incluir los parámetros adecuados o para extender la cabecera de los mensajes SOAP de nuevo con parámetros de cabecera adecuados.
2. Las aplicaciones que buscan autenticación necesitan implementar un esquema de autenticación en base al esquema proporcionado por el operador como se describió en el paso 1.

a. Las credenciales para autenticar abonados del operador se generan en base a secretos comunes conocidos tanto por el operador como por la aplicación (por ejemplo, la id del sistema del usuario, datos de terminal, etc.).
b. Las credenciales para autenticar no abonados necesitan ser acordadas por adelantado. Esto puede ocurrir a través de registro en sitios adecuados proporcionados por el operador.

A continuación, se describirá una realización de un mecanismo de autenticación que se puede usar en combinación con el mecanismo de correspondencia de sesión anterior. Como entrada, el mecanismo recibe mensajes de solicitud de invocación entrantes desde las aplicaciones no SIP que se ejecutan por ejemplo, en terminales fuera del dominio IMS. La salida será el estado de autenticación de las aplicaciones no SIP.

1. Analizar la dirección IP de la solicitud entrante

a. Las solicitudes que se originan desde direcciones dentro del dominio de confianza (desde el operador en sí mismo o desde otras redes de confianza) se procesan además en el paso 2.
b. Las solicitudes que se originan desde fuera del dominio de confianza se procesan además en el paso 4.

2. SI la dirección IP es la dirección de un nodo conocido y de confianza que añade credenciales de autenticación a la solicitud (por ejemplo, una pasarela WAP)

a. ENTONCES SI las credenciales incorporadas están disponibles (por ejemplo, en el caso de una comprobación de pasarela WAP para cabecera HTTP especial insertada por la pasarela WAP)

i ENTONCES Analizar las credenciales (por ejemplo, extraer el número MSISDN)

ii DE OTRO MODO ir al paso 3

b. DE OTRO MODO ir al paso 3

3. Analizar la solicitud (por ejemplo, sobre SOAP) y comprobar la disponibilidad de credenciales de autenticación (por ejemplo, dentro de la cabecera/cuerpo SOAP)

a. SI las credenciales están disponibles entonces quitar los datos de autenticación requeridos por el dispositivo de correspondencia a partir de la solicitud a fin de cumplir con la API de servicio original. Proceder con una autenticación adicional en base a estos datos en el paso 5.
Los siguientes ejemplos ilustran cómo se extraen las credenciales requeridas para establecer la sesión IMS a partir del mensaje SOAP extendido entrante produciendo por ello un mensaje SOAP no extendido.
Un ejemplo de solicitud SOAP extendida con credenciales de autenticación se da más adelante:

```
<soap:Envelope xmlns:soap=http://www.w3.org/2002/06/soap-envelope
  xmlns:auth = "http://liberty.org">
<soap:Header>
  <auth:credential1 name="user1"/>
  <auth:credential2:password="secret"/>
   </soap:Header>
   <soap:Body>
      <!-- Application Payload
         MMService specific payload -->
   </soap:Body>
</soap:Envelope>
```

Un ejemplo de solicitud SOAP sin credenciales de autenticación se da más adelante:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2002/06/soap-envelope">
   <soap:Header>
   </soap:Header>
   <soap:Body>
      <!-- Application Payload
         MMService specific payload -->
   </soap:Body>
</soap:Envelope>
```

b. DE OTRO MODO ir al paso 4

4. Usar las propiedades de dirección del paquete entrante (por ejemplo, dirección IP, dirección DNS, dirección MAC, etc.) para determinar implícitamente la id del sistema del usuario y crear las credenciales temporales adecuadas. Se debería señalar que esta identificación no es tan precisa y segura como la identificación permitida a través de los pasos previos. La falta de precisión se puede atribuir por ejemplo a la falta de correspondencia única entre las direcciones IP y las aplicaciones.

5. Convertir las credenciales a formato IMS, usarlas para autenticar la aplicación

A continuación, se tratarán en más detalle algunas realizaciones de dispositivos de correspondencia 100.

Según una realización mostrada en la Figura 4, el dispositivo de correspondencia 100 se implementa como un nodo pasarela situado entre el dominio IMS 10 y clientes 20 situados en el dominio no IMS (por ejemplo, clientes SOAP 20 que usan Servicios Web). La Figura 4 ilustra una correspondencia de sesión de tiempo de ejecución no SIP a SIP para acceder a servicios controlados por operador no SIP desplegados dentro del dominio IMS 10.

El Protocolo de Descripción de Servicio (SDP) se puede usar para describir diferentes tipos de servicios SIP. Cada inicio de sesión SIP puede contener una descripción SDP. Una posibilidad por lo tanto sería definir descripciones SDP para establecer sesiones de un tipo específico que corresponden a invocaciones de servicio no IMS específicas

y tecnología de establecimiento/gestión de sesión. La correspondencia/conversión de sesión también se puede permitir de esta manera asignando ciertos campos de invocaciones de servicio entrantes a sus campos correspondientes en la descripción SDP. En este caso se asignarían tipos específicos de invocaciones de servicio no IMS (por ejemplo, servicios CORBA, servicios J2EE, servicios RMI de Java, servicios .NET y naturalmente servicios SOAP puros) a descripciones SDP predefinidas específicas para estas tecnologías.

La correspondencia de sesión se puede implementar usando una tabla que enumera las sesiones en marcha actualmente. En la tabla, cada sesión en marcha se puede asociar con parámetros particulares que permiten al dispositivo de correspondencia 100, tras una recepción de un mensaje de capa de servicio desde los clientes 20, identificar si el mensaje se refiere o no a una sesión en marcha dentro del dominio IMS 10. En principio, un cliente individual 20 se puede asociar con la pluralidad de sesiones individuales que implican uno y el mismo servicio o diferentes servicios dentro del dominio IMS 10.

Como se muestra en la Figura 4, se recibe un mensaje de invocación de servicio por el dispositivo de correspondencia 100 en una capa de servicio (SOAP sobre HTTP) y reconoce como que invoca un servicio dentro del dominio IMS 10. Entonces, en una capa de control de sesión (“capa SIP”), tiene lugar una conversión de elemento de protocolo dentro del dispositivo de correspondencia 100 en contexto con proporcionar una sesión de control IMS (“sesión controlada por SIP”) para el servicio a ser invocado. La sesión de control IMS se usa entonces como vehículo para comunicación entre el cliente 20 y el servicio solicitado dentro del dominio IMS 20.

En el escenario de la Figura 4, el dispositivo de correspondencia 100 es completamente transparente a los clientes SOAP 20 que invocan (es decir, los clientes 20 no necesitan tener ningún conocimiento de la presencia y función del dispositivo de correspondencia 100). Esto es ventajoso debido a que permite el uso por clientes 20 estándar (no modificados) en un dominio no IMS.

El dispositivo de correspondencia 100 también se puede implementar en el lado del dominio no IMS, por ejemplo, dentro del cliente 20 modificando las pilas de protocolo de cliente (es decir, J2EE, pila SOAP de WS, etc.). Esto se representa en la Figura 5 usando Servicios Web como ejemplo.

La Figura 5 ilustra una correspondencia de sesión de tiempo de ejecución no SIP o SIP para acceder a servicios controlados por operador no SIP desplegados dentro del dominio IMS 10. En este escenario, el dispositivo de correspondencia 100 se integra en la pila de protocolo de cliente del cliente 20 en el dominio no IMS. Esta solución es particularmente ventajosa debido a que no requiere el despliegue de nodos de red adicionales (por ejemplo, de pasarelas como en la realización mostrada en la Figura 4).

Dada la falta de clientes habilitados IMS extendidos (por ejemplo, terminales de usuario tales como teléfonos móviles) en el mercado, tal pila modificada se podría implementar directamente en la primera generación de tales clientes. Esto es una ventaja en la medida que elimina costes relacionados con actualización comparado con escenarios de despliegue típicos que requieren que clientes existentes sean actualizados con una funcionalidad adicional.

La implementación del dispositivo de correspondencia 100 como una pasarela se usa normalmente para acceso transparente a los servicios controlados por operador dentro del dominio IMS 10.Un caso de uso especial para la solución basada en pasarela podría ser la situación donde dos componentes no IMS 20, 30 comunican uno con otro a través de tal pasarela 100 para ser capaces de utilizar servicios IMS en forma de funciones de soporte proporcionadas por el dominio IMS 10 (tales como AAA, HSS, etc., usando el protocolo DIAMETER). Este escenario se muestra en la Figura 6 y es particularmente interesante para proveedores de servicios de terceras partes, ya que consideran que el operador es un mediador fiable y digno de confianza. El operador, a su vez, también puede beneficiarse ya que puede tarificar por proporcionar esta funcionalidad.

El escenario mostrado en la Figura 6 puede requerir que un proveedor de servicios 30 en un dominio no IMS tenga un acuerdo de negocio adecuado con el operador IMS y haya desplegado su servicio de un modo que se registre y sea accesible a través de la pasarela del dispositivo de correspondencia 100. Alternativamente, un cliente 20 en un dominio no IMS también se puede registrar con el operador. Esto permite al cliente 20 beneficiarse de los mecanismos de autenticación y autorización SIP proporcionados por el operador para identificarse por sí mismo hacia el proveedor de servicios de terceras partes 30.

Con referencia a la Figura 7, se describirá una realización de un esquema de invocación de direccionamiento y servicio uniforme basado en SIP que se puede usar en combinación con las realizaciones anteriores.

En lugar de usar el URL de HTTP (Protocolo de Transferencia de Hipertexto), los URI de SIP lógicos (y eventualmente los URL de SIP) se usan para el esquema de direccionamiento uniforme y para invocaciones de servicio móvil. El acceso al servicio a través de URI permite movilidad de servicio proporcionando un acceso transparente al servicio con independencia de su URL actual. Esto permite el direccionamiento de servicios IMS desplegados en dispositivos móviles que no tienen un acoplamiento fijo a la red y consecuentemente que no tiene un URL fijo.

El escenario mostrado en la Figura 7 implica dos pasos principales, esto es

a. definir el uso de un URI de SIP para invocación dinámica de servicios IMS móviles con independencia de su URL actual. (Posiblemente definiendo una extensión para Direccionamiento de WS.)
b. definir el direccionamiento fijo de servicios que usan un URL de SIP

Como se ha mostrado en las realizaciones anteriores, la interoperabilidad entre el IMS y cualquier otro dominio se puede aumentar estableciendo una correspondencia entre una sesión/servicio de WS y (una o múltiples) sesiones SIP. En este contexto, los elementos SOAP usados para transportar la información de sesión se pueden convertir en cabeceras SIP y viceversa. Se puede evitar el reenvío de la información relacionada con la sesión de WS en los mensajes SOAP dentro de redes IMS/SIP si la sesión SIP ya se ha dotado con ella.

Las técnicas se pueden realizar por una pasarela SIP a no SIP (por ejemplo, SIP-SOAP) que asigna transparentemente entre por ejemplo servicios no SIP y sesiones SIP y se puede usar sin adaptación de la aplicación cliente. Alternativamente, las técnicas se realizan en las realizaciones anteriores extendiendo la pila WS/pila SIP para mejorar las aplicaciones permitiéndolas asignar transparentemente entre sesiones WS y sesiones SIP sin componentes de infraestructura adicionales en la red.

De esta manera, las realizaciones proporcionan invocación de WS dentro de un dominio o red IMS. Permiten el uso de mecanismos existentes de gestión de sesión basada en SIP más eficientes para gestión de sesión WS y proporcionan una mejor interoperabilidad e integración entre el sistema IMS y la infraestructura y los Servicios Web desplegados dentro del dominio IMS. Además, las realizaciones hacen posible usar mecanismos IMS estándar para AAA, tarificación, etc. también para invocaciones y control de servicios tales como Servicios Web fuera del dominio IMS. Haciéndolo así, las realizaciones permiten una integración sin discontinuidad de Servicios Web en sistemas IMS. Los desarrolladores no necesitan soportar explícitamente los protocolos IMS/SIP y las API. Todo esto se puede hacer transparentemente o por las extensiones de pilas WS y/o SIP.

Además, las realizaciones permiten una reducción en la cantidad de tráfico requerido para transmisión de información de sesión por ejemplo, mediante Servicios Web dentro de redes IMS. Las realizaciones también proporcionan Servicios Web con movilidad permitiendo invocación que usa su URI que puede ser diferente de su URL. Esto permite al servicio cambiar su plataforma de ejecución (y por lo tanto su URL) mientras que aún se puede direccionar bajo el mismo URI. A este respecto, el encaminamiento de llamadas de invocación de servicio se puede manejar por un registro SIP (es decir, un nodo CSCF en el dominio IMS) que es consciente de la posición actual de cada usuario y redirige llamadas de invocación de servicio usando el URI de SIP al URL de SIP correcto actualmente.

Se debería señalar que los planteamientos expuestos anteriormente se pueden usar no solamente para correspondencia de sesiones de Servicios Web a sesiones SIP. En principio, la invención se puede usar para correspondencia de cualquier protocolo de Llamada de Procedimiento Remoto (RPC) que tiene el concepto de sesiones a cualquier protocolo interno IMS adecuado para las necesidades requeridas. Estos pueden incluir, por ejemplo, CORBA, RMI de Java y otros protocolos propietarios.

Aunque la presente invención se ha descrito con respecto a realizaciones particulares, los expertos en la técnica reconocerán que la presente invención no está limitada a las realizaciones específicas descritas e ilustradas en la presente memoria. Por lo tanto, aunque la presente invención se ha descrito en relación a sus realizaciones preferidas, se tiene que entender que esta descripción es solamente ilustrativa. Por consiguiente, se pretende que la invención esté limitada solamente por el alcance de las reivindicaciones adjuntas a la misma.

REIVINDICACIONES

1. Un método de provisión de interoperabilidad entre un dominio de subsistema multimedia de protocolo de Internet (IMS) (10) y un domino no IMS (20), que comprende los pasos de:

recibir (S1) en una capa de servicio un mensaje de invocación de servicio (101) desde el dominio no IMS;
analizar (S2) el mensaje para identificar (S3) el mensaje (101) como una solicitud para invocar un servicio dentro del dominio IMS;
convertir (S4) en una capa de control de sesión elementos de protocolo de control de sesión no IMS relacionados con el mensaje (101) en elementos de protocolo relacionados con control de sesión IMS;
enviar (S5) uno o más mensajes (107) hacia el dominio IMS para proporcionar una sesión de control IMS en el dominio IMS en base a los elementos de protocolo relacionados con control de sesión IMS; y
reenviar en la capa de servicio el mensaje de invocación de servicio (107) usando la sesión de control IMS;
caracterizado por que además comprende los pasos de:

analizar el mensaje (101, 107) recibido desde el dominio no IMS y/o desde el dominio IMS;
determinar un estado de la sesión con el servicio en el dominio IMS en base al mensaje analizado; y
almacenar el estado de la sesión.

2. El método de la reivindicación 1, que además comprende el paso de:

recibir un mensaje adicional (101) desde el dominio no IMS relacionado con el servicio invocado dentro del dominio IMS; y
reenviar en la capa de servicio el mensaje de servicio (107) usando la sesión de control IMS.

3. El método de cualquier reivindicación precedente, que además comprende los pasos de:

recibir un mensaje (107) desde el dominio IMS durante la sesión;
convertir elementos de protocolo de control de sesión IMS relacionados con el mensaje (107) del dominio IMS en elementos de protocolo de control de sesión no IMS;
generar un mensaje no IMS (101) en base a los elementos de protocolo de control de sesión no IMS; y
enviar el mensaje no IMS (101) al dominio no IMS.

4. El método de la reivindicación 3, en donde el mensaje no IMS se envía al dominio no IMS durante la sesión.

5. El método de cualquier reivindicación precedente, en donde el servicio en el dominio IMS es una función de soporte IMS, tal como autenticación, autorización y contabilidad, tarificación, control de acceso o HSS.

6. El método de cualquier reivindicación precedente, en donde el servicio en el dominio IMS es una aplicación basada en protocolo no IMS.

7. El método de cualquier reivindicación precedente, en donde los elementos de protocolo de control de sesión IMS comprenden cabeceras de protocolo de inicio de sesiones (SIP) y los elementos de protocolo de control de sesión no IMS comprenden cabeceras no SIP.

8. El método de cualquier reivindicación precedente, en donde el dominio no IMS emplea un protocolo para intercambiar mensajes basados en Leguaje de Marcas (ML).

9. El método de cualquier reivindicación precedente, que comprende los pasos de:

comprobar si una sesión con el servicio en el dominio IMS está en marcha; y
si no hay ninguna sesión en marcha, iniciar una nueva sesión bajo el protocolo de control de sesión IMS.

10. El método de cualquier reivindicación precedente, que además comprende el paso de asociar un solicitante de servicio con una o más sesiones solicitadas y/o en marcha dentro del dominio IMS.

11. El método de la reivindicación 10, en donde el solicitante de servicio es una aplicación o un componente de red fuera del dominio IMS.

12. El método de cualquier reivindicación precedente, que comprende el paso de:

autenticar el mensaje no IMS anterior a establecer la sesión de control en el dominio IMS.

13. El método de la reivindicación 12, en donde el paso de autenticación del mensaje no IMS comprende analizar una dirección especificada en el mensaje.

14. El método de cualquier reivindicación precedente, que comprende el paso de:

emplear un esquema de direccionamiento uniforme usando direccionamiento SIP para la invocación de servicios fijos y/o móviles.

15. El método de cualquier reivindicación precedente, en donde el servicio a ser invocado reside en una plataforma móvil dentro del dominio IMS, el método que comprende el paso de:

definir un identificador de recursos único (URI) de SIP para invocación dinámica del servicio en el dominio IMS, con independencia de un localizador de recursos único (URL) actual para la plataforma móvil.

16. El método de cualquier reivindicación precedente, que comprende el paso de:

definir un localizador de recursos único (URL) de SIP para direccionamiento fijo del servicio en el dominio IMS.

17. Un producto de programa de ordenador que comprende partes de código de programa para realizar los pasos de cualquiera de las reivindicaciones precedentes cuando el producto de programa de ordenador se ejecuta en uno o más ordenadores o sistemas informáticos.

18. El producto de programa de ordenador de la reivindicación 17, en donde el producto de programa de ordenador se almacena en un medio de grabación legible por ordenador.

19. Un sistema que comprende un procesador de ordenador y una memoria acoplada al procesador, en donde la memoria se codifica con uno o más programas que pueden realizar pasos para proporcionar interoperabilidad entre un protocolo de inicio de sesiones y un no protocolo de inicio de sesiones según cualquiera de los métodos de las reivindicaciones 1 a 16.

20. Un dispositivo de correspondencia (100) para proporcionar interoperabilidad entre un dominio de protocolo de inicio de sesiones (IMS) y un dominio no IMS (20), que comprende:

una unidad de análisis (102) para analizar mensajes de invocación de servicio entrantes (101) recibidos en una capa de servicio desde el dominio no IMS (20), para identificar si uno de los mensajes de invocación de servicio (101) es una invocación de un servicio dentro del dominio IMS (10);
una unidad de conversión (104) para convertir en una capa de control de sesión elementos de protocolo de control de sesión no IMS relacionados con uno de los mensajes (101) en elementos de protocolo relacionados con control de sesión IMS; y
una unidad de mensajería (106) para generar uno o más mensajes (107) para proporcionar una sesión de control IMS en el dominio IMS (10) en base a los elementos de protocolo relacionados con control de sesión IMS;
en donde el dispositivo (100) está adaptado para reenviar en la capa de servicio el mensaje de invocación de servicio usando la sesión de control IMS;
caracterizado por que el dispositivo (100) está adaptado además para
analizar el mensaje (101, 107) recibido desde el dominio no IMS y/o desde el dominio IMS;
determinar un estado de la sesión con el servicio en el dominio IMS en base al mensaje analizado; y
almacenar el estado de la sesión.

21. El dispositivo de correspondencia (100) de la reivindicación 20, en donde el dispositivo se implementa como una pasarela entre el dominio IMS y el dominio no IMS.

22. El dispositivo de correspondencia (100) de la reivindicación 20, en donde el dispositivo está integrado en una pila de protocolo de un componente de red en el dominio no IMS.

23. Un terminal de usuario que comprende el dispositivo de correspondencia (100) de cualquiera de las reivindicaciones 20 a 22.

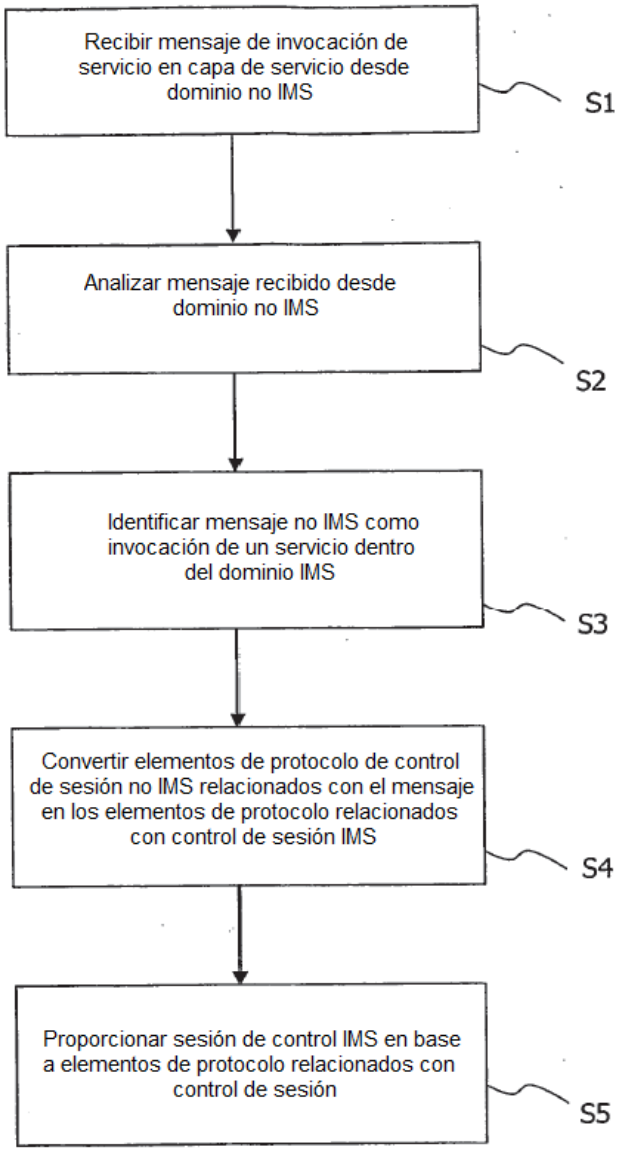
Recibir mensaje de invocación de servicio en capa de servicio desde dominio no IMS
S1
Analizar mensaje recibido desde dominio no IMS
S2
Identificar mensaje no IMS como invocación de un servicio dentro del dominio IMS
S3
Convertir elementos de protocolo de control de sesión no IMS relacionados con el mensaje en los elementos de protocolo relacionados con control de sesión IMS
S4
Proporcionar sesión de control IMS en base a elementos de protocolo relacionados con control de sesión
S5

Fig. 1

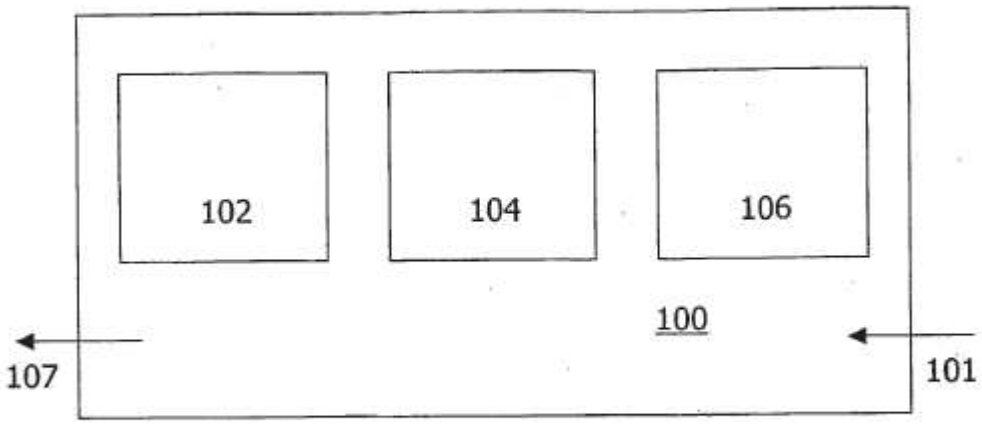

Fig. 2

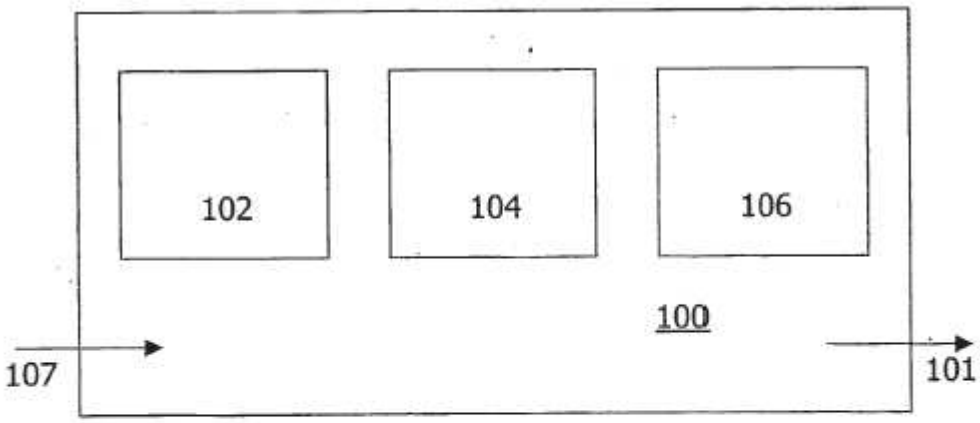

Fig. 3

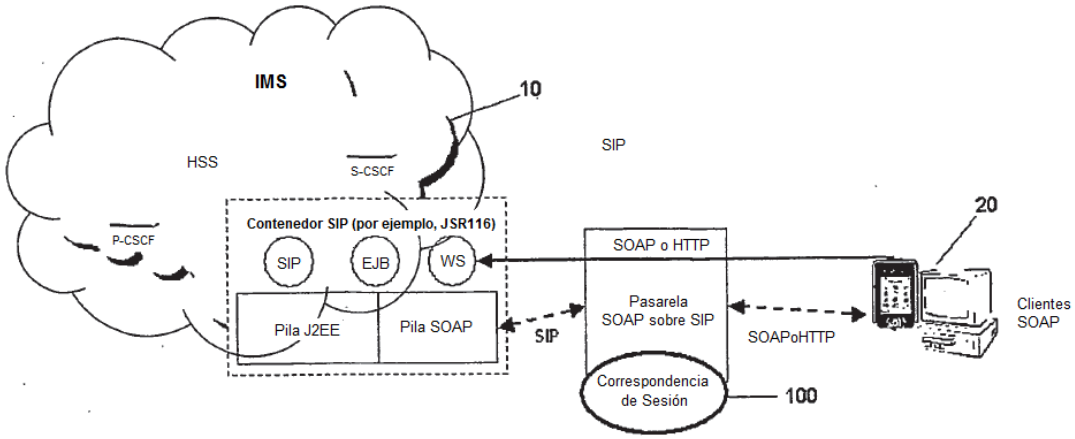
IMS
10
SIP
HSS
S-CSCF
P-CSCF
Contenedor SIP (por ejemplo, JSR116)
SIP
EJB
WS
Pila J2EE
Pila SOAP
SIP
SOAP o HTTP
Pasarela
SOAP sobre SIP
SOAPoHTTP
20
Clientes
SOAP
Correspondencia
de Sesión
100

Fig. 4

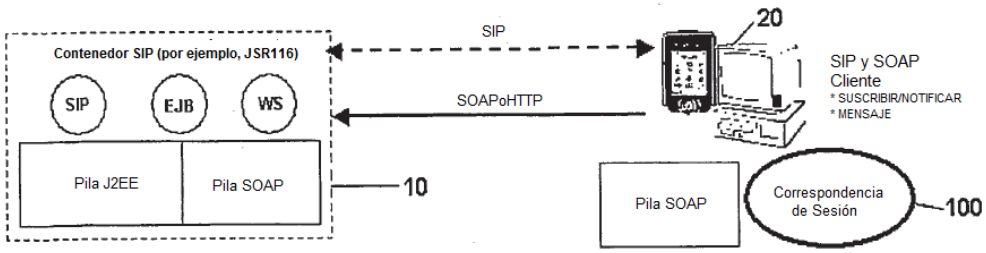
Contenedor SIP (por ejemplo, JSR116)
SIP
EJB
WS
Pila J2EE
Pila SOAP
10
SIP
SOAPoHTTP
20
SIP y SOAP
Cliente
* SUSCRIBIR/NOTIFICAR
* MENSAJE
Pila SOAP
Correspondencia
de Sesión
100

Fig. 5

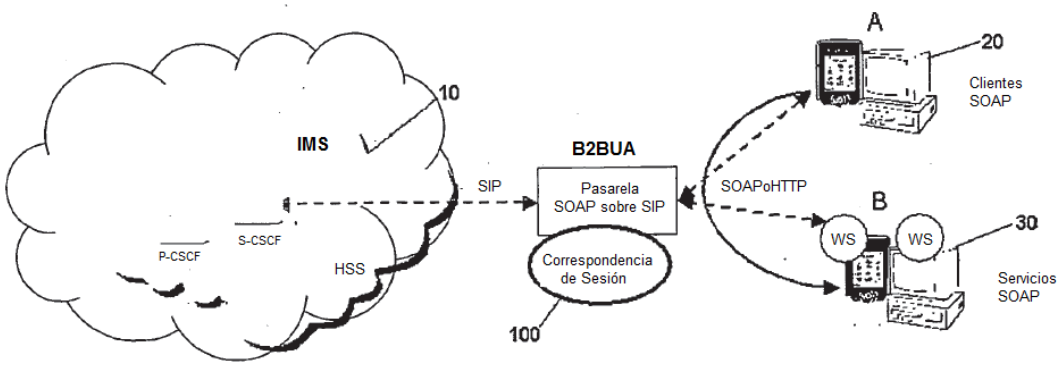
IMS
10
P-CSCF
S-CSCF
HSS
SIP
B2BUA
Pasarela
SOAP sobre SIP
Correspondencia
de Sesión
100
SOAPoHTTP
A
20
Clientes
SOAP
B
WS
WS
30
Servicios
SOAP

Fig. 6

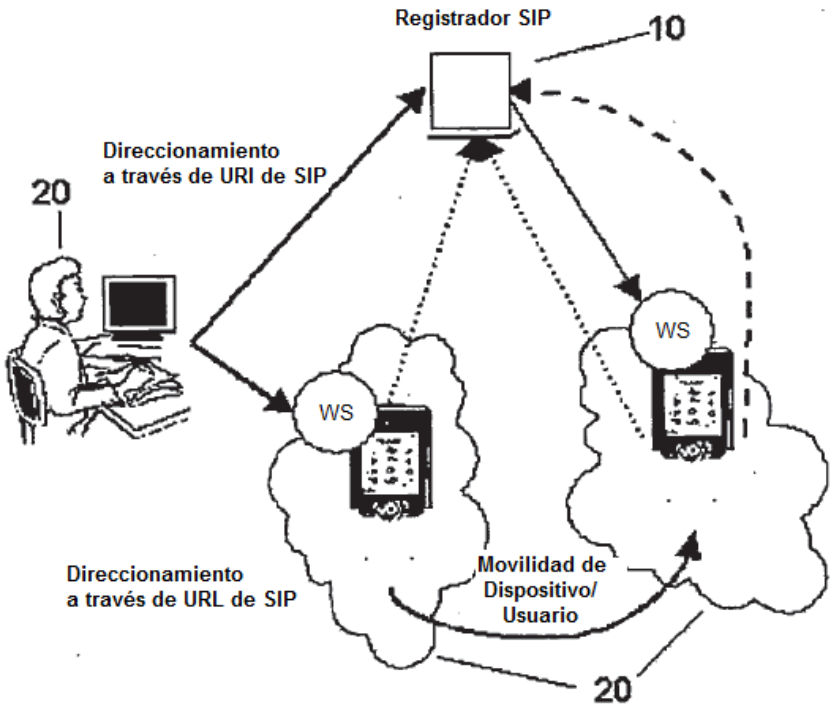
Registrador SIP
10
Direccionamiento
a través de URI de SIP
20
WS
WS
Direccionamiento
a través de URL de SIP
Movilidad de
Dispositivo/
Usuario
20

Fig. 7