(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 522 621**

(51) Int. CI.:

H04W 8/12 (2009.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.10.2008 E 08839268 (3)**

(97) Fecha y número de publicación de la concesión europea: **13.08.2014 EP 2204055**

(54) Título: **Intermediario de itinerancia**

(30) Prioridad:

18.10.2007 EP 07118799

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.11.2014

(73) Titular/es:

NOKIA SOLUTIONS AND NETWORKS OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

KAPPLER, CORNELIA;
PAMPU, CORNEL y
TIONARDI, LAURENSIUS

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

INTERMEDIARIO DE ITINERANCIA

DESCRIPCIÓN

Campo de la invención

La presente invención se refiere a un aparato y a un método que realizan funcionalidades de un intermediario de itinerancia.

Antecedentes de la técnica relacionada

La técnica anterior que está relacionada con este campo puede encontrarse en el documento "Cornelia Kappler *et al.*: 'A Framework for Self-organized Network Composition' AUTONOMIC COMMUNICATION LECTURE NOTES IN COMPUTER SCIENCE; LNCS, Springer-Verlag, BE, vol. 3457, 2005, páginas 139-151". Este documento da a conocer un marco para un plano de control autoorganizado, flexible, para redes móviles y universales futuras. Las redes compuestas se denominan redes de entorno que usan una interfaz específica (interfaz de red de entorno) para comunicarse entre sí.

Se da a conocer una técnica anterior adicional en el documento "O. Salazar; P. Martins; J. Demerjian; S. Tohmé: 'Enabling Roaming in Heterogeneous Multi-Operator Wireless Networks', Journal of Communications (JCM), vol. 2, n.º 4, 30 de junio de 2007, páginas 18-28. Este documento da a conocer el establecimiento de una confianza mutua entre operadores de red celular y redes inalámbricas sin licencia a través de una monitorización y cumplimiento de SLA (acuerdo de nivel de servicio) eficaces y un control de acceso basado en intermediarios.

La itinerancia es una funcionalidad importante soportada en redes móviles. Significa que un abonado de una primera red (su red doméstica) puede alcanzarse en otra (segunda) red (la red visitada). En otras palabras, un abonado puede usar su terminal móvil también cuando está fuera de la cobertura de su red doméstica.

La red visitada y la red doméstica están conectadas habitualmente por una red principal, el GRX (intercambio de paquetes de GPRS; GPRS: servicio general de radio por paquetes) o el IPX (intercambio de IP; IP: protocolo de Internet). Por tanto, el tráfico debido a la itinerancia se desplaza desde la red visitada a través del GRX (o IPX) hasta la red doméstica.

Las siguientes son las acciones típicas realizadas, cuando un abonado itinerante usa una red visitada. En primer lugar, se autentica y autoriza el abonado itinerante basándose en la información ubicada en su red doméstica. Es decir, el elemento de red apropiado en la red visitada tal como un SGSN (nodo de soporte de GPRS de servicio) o un servidor proxy de AAA (autenticación, autorización y contabilidad) extrae información y decisiones desde el elemento correspondiente en la red doméstica, por ejemplo desde un HLR (registro de localización de abonados) o un servidor de AAA. A continuación, el abonado itinerante se prepara para enviar datos. En muchos casos, esto implica establecer un túnel con la red doméstica. Por ejemplo, éste podría ser un túnel IPsec (protocolo de Internet seguro) entre un encaminador de acceso y una pasarela de datos por paquetes (PDG) o un túnel de GTP (protocolo de túnel de GPRS) entre SGSN y un GGSN (nodo de soporte de GPRS de pasarela), si el GGSN está ubicado en la red doméstica. Entonces, la facturación y el cobro se realizan mediante la red doméstica basándose en la información recopilada tanto en la red visitada como en la red doméstica.

Evidentemente, la red doméstica y la red visitada requieren una relación contractual con el fin de que la red visitada acepte los abonados de itinerancia. Estos contratos se denominan acuerdos de itinerancia (RoA). Los acuerdos de itinerancia pueden establecerse entre redes de muchas tecnologías, es decir redes móviles terrestres públicas (PLMN) según el 3GPP (proyecto de asociación de 3ª generación) tal como UMTS (servicio universal de telecomunicaciones móviles) y redes de no 3GPP tales como WLAN (redes de área local inalámbricas).

Como tal, los acuerdos de itinerancia son unidireccionales, es decir definen una relación de itinerancia entre una red doméstica y una red visitada. Habitualmente, sin embargo, dos redes negocian un par recíproco de acuerdos de itinerancia, en los que acuerdan aceptar abonados itinerantes entre sí.

Los acuerdos de itinerancia se establecen en un proceso de dos fases que, convencionalmente, se realiza de manera manual.

En primer lugar, se negocia un contrato jurídicamente vinculante.

En segundo lugar, se intercambia información de configuración y luego se configuran los elementos de red implicados en tratar con abonados itinerantes según los requisitos de contrato y de conexión. Esta segunda etapa de configuración implica lo siguiente. Como información de configuración, se intercambia la información de direccionamiento tales como las direcciones IP de los elementos de red que envían tráfico a la otra red, por ejemplo servidores (proxy) de AAA, SGSN, GGSN y DNS (servidor de nombres de dominio). Otra información intercambiada puede incluir el nombre del proveedor de GRX, la pasarela de SCCP (parte de control y conexión de señalización)

internacional, la estructura de IMSI (identidad de abonado móvil internacional), la estructura de MSISDN (número de red digital de servicios integrados de abonado móvil), las versiones de protocolo (protocolo de túnel de GPRS, parte de aplicación móvil,...), etc.

Además, puede ser necesario que se realicen los siguientes ejemplos de configuraciones. Los cortafuegos y las pasarelas de borde deben estar configurados de manera que dejen pasar tanto el tráfico de señalización (por ejemplo, consultas de DNS, GTP, MAP, RADIUS, Diameter,...) como el tráfico de plano de usuario. Deben habilitarse los elementos de red en las dos redes para que se localicen entre sí (por ejemplo, el servidor proxy de AAA debe localizar el servidor de AAA, el SGSN debe localizar el HLR y el GGSN, y el encaminador de acceso debe localizar la pasarela de acceso de WLAN, etc.). La información de localización puede configurarse de manera estática (por ejemplo, en el encaminador de acceso) o puede recuperarse a través del DNS. En este caso, se proporciona al servidor DNS en la red visitada una entrada que señala al servidor DNS en la red doméstica. Además, en caso de HLR, es necesario que cada operador de PLMN informe a sus portadoras de SCCP y proveedores de GRX de modo que puedan encaminar y filtrar correctamente el tráfico de itinerancia.

Convencionalmente, se establecen acuerdos de itinerancia de una manera bilateral. Es decir, dos redes acuerdan un acuerdo de itinerancia o un par de acuerdos de itinerancia recíprocos. Sin embargo, el número de acuerdos de itinerancia puede volverse bastante grande, y su establecimiento y mantenimiento pueden ser bastante costosos.

Este problema se aborda mediante el concepto de intermediarios de itinerancia (RB). El intermediario de itinerancia soporta el establecimiento de un acuerdo de itinerancia multilateral tal como se ilustra en la figura 1. Un RB visitado (VRB) establece varias ramas visitadas de un acuerdo de itinerancia con varias redes visitadas. El VRB está enlazado a un RB doméstico (HRB), en el que naturalmente también pueden estar coubicados el HRB y el VRB. Entonces, la red doméstica y el HRB establecen la rama doméstica del acuerdo de itinerancia. Esto conduce automáticamente a un acuerdo de itinerancia multilateral de la red doméstica con todas las (o un subconjunto de las) redes visitadas con las que el VRB tenga un contrato. En otras palabras, la red doméstica tiene el mismo contrato con todas las redes visitadas, sin la posibilidad de diferenciar entre las mismas.

Cuando están implicados intermediarios de itinerancia, las redes visitadas (en el caso de una PLMN, una “VPLMN”) son, en gran medida, invisibles para las redes domésticas (en caso de una PLMN, una “HPLMN”), puesto que todo el tráfico se redirige mediante proxy por el RB, y la mayoría de las transacciones empresariales (con la posible excepción de facturación) se realizan con el RB. Desde la perspectiva de la HPLMN, el RB es básicamente la VPLMN. En otras palabras, a los acuerdos de itinerancia intermediados les falta lo que se denomina transparencia.

La asociación GSM (GSMA) especifica el GRX, el IPX y los detalles de establecimiento de acuerdo de itinerancia se especifican mediante.

Sumario de la invención

Por tanto, un objeto de la presente invención es mejorar la tecnología de la técnica anterior.

Según la presente invención, esto se consigue mediante el contenido definido en las reivindicaciones independientes.

Se exponen modificaciones ventajosas de la misma en las reivindicaciones dependientes.

Con la presente invención, es posible establecer acuerdos de itinerancia individualizados intermediados por un intermediario de itinerancia. Además, puede aumentarse significativamente la transparencia de acuerdos de itinerancia intermediados. En comparación con la técnica anterior, se aumenta además el grado de automatización. Además, con respecto a un acuerdo de itinerancia ya establecido y configurado, según la presente invención, es posible de una manera más fácil cualquier cambio, incluso incluyendo la finalización tal como con respecto a la configuración, también mediante una automatización alta.

Breve descripción de los dibujos

Aspectos, características y ventajas adicionales de la presente invención resultarán evidentes de manera más completa a partir de la siguiente descripción detallada de las realizaciones preferidas, cuando se toman junto con los dibujos adjuntos, en los que:

la figura 1 muestra un acuerdo de itinerancia multilateral establecido a través de un HRB y un VRB según la técnica anterior;

la figura 2 muestra acuerdos de itinerancia individualizados establecidos a través de HRB y VRB avanzados según una primera realización de la presente invención;

la figura 3 muestra una vista de componentes detallada del intermediario de itinerancia avanzado según la primera

realización de la presente invención incluyendo una ilustración del proceso para establecer un acuerdo de itinerancia individualizado;

la figura 4 muestra una arquitectura de red con proxy de NICO y pasarela de NICO para el ejemplo de un acuerdo de itinerancia bilateral según una segunda realización de la presente invención;

la figura 5 muestra la estructura interna de una pasarela de NICO así como un proceso correspondiente para establecer un acuerdo de itinerancia transparente, intermediado con la ayuda de pasarela de NICO y proxy de NICO según la segunda realización de la presente invención;

la figura 6 muestra la arquitectura interna de la pasarela de NICO según la segunda realización de la presente invención en más detalle; y

la figura 7 muestra la arquitectura interna del proxy de NICO según la segunda realización de la presente invención.

Descripción detallada de las realizaciones preferidas

A continuación, se realizará una descripción de las que se consideran actualmente las realizaciones preferidas de la presente invención. Sin embargo, se entiende que la descripción se proporciona sólo a modo de ejemplo, y que las realizaciones descritas no deben entenderse de ningún modo como que limitan la presente invención a las mismas.

Por ejemplo, la presente invención puede aplicarse a redes móviles tales como PLMN, pero también a otras redes móviles tales como WLAN (red de área local inalámbrica) y WIMAX (interoperabilidad mundial para acceso por microondas).

Incluso para redes fijas, la presente invención podría aplicarse donde, por ejemplo, los servicios proporcionados fuera de la red fija deban estar disponibles para los usuarios de la red fija de modo que los usuarios puedan “itinerar” a estos servicios proporcionados “fuera”. Por tanto, también en estos casos será necesario un acuerdo de itinerancia y puede aplicarse la presente invención de una manera beneficiosa.

No obstante, a continuación la presente invención se describe a modo de ejemplo con respecto a PLMN. Sin embargo, tal como se indicó anteriormente, la presente invención no se limita a la misma.

Primera realización

Con respecto a los acuerdos de itinerancia intermediados convencionalmente, se considera según la primera realización de la presente invención que el operador de red doméstica tiene demasiado poco control sobre la red visitada con la que va a tener un acuerdo de itinerancia. Es decir, el acuerdo de itinerancia se establece con todas o, en algunos casos, un subconjunto de redes visitadas afiliadas con el VRB. Además, se reduce la flexibilidad con respecto a los términos y condiciones de los acuerdos de itinerancia multilaterales en comparación con los acuerdos de itinerancia bilaterales. Además, el proceso de establecimiento manual se considera costoso.

Para superar estos problemas, con la primera realización de la presente invención, la red doméstica y la(s) red(es) visitada(s) están implicadas en la decisión y configuración del acuerdo de itinerancia intermediado por intermediarios de itinerancia avanzados. El resultado es un acuerdo de itinerancia individualizado que puede ser bilateral o multilateral, es decir establecerse entre una HPLMN y varias VPLMN o viceversa.

A continuación, esto se describe en más detalle.

Haciendo referencia de nuevo a la figura 1, el VRB mantiene múltiples acuerdos de itinerancia de “una rama” (línea gruesa resaltada) con redes visitadas W, X, Y, Z y el HRB mantiene la rama doméstica con la red doméstica. El objeto de la invención no es cómo se establecen estas ramas.

Sin embargo, una vez que las ramas están en su lugar, no se establece automáticamente un acuerdo de itinerancia multilateral. Más bien, la red doméstica y la red visitada determinan qué acuerdos de itinerancia bilaterales o multilaterales deben establecerse, intermediados por los intermediarios de itinerancia. También es posible individualizar algunos parámetros del acuerdo de itinerancia en esta fase, por ejemplo tarifas entre operadores (IOT) o servicios ofrecidos.

En la figura 2 se ilustra un posible resultado. La red doméstica tiene un acuerdo de itinerancia bilateral (línea gruesa resaltada) con la red X, con términos y condiciones específicos para la red X, y un acuerdo de itinerancia multilateral, diferente (línea gruesa discontinua) con las redes Y y Z. La red doméstica no tiene un acuerdo de itinerancia (línea discontinua delgada) con la red W.

Esto se consigue con intermediarios de itinerancia avanzados según la primera realización de la presente invención con los que pueden implementarse varios grados de flexibilidad y automatización. Por ejemplo:

(1) Pueden realizarse automáticamente ambas fases de establecimiento de acuerdo de itinerancia.

(2) Se automatiza la fase de configuración en los intermediarios de itinerancia.

(3) Las redes pueden elegir su red de socios de itinerancia en un proceso en línea, por ejemplo a través de una interfaz web con el RB.

A continuación se describe un posible ejemplo de implementación de una combinación de versiones (2) y (3), que se ilustra en la figura 3. En el presente documento, se supone una coubicación de HRB y VRB, y que las redes de PLM que establecen el acuerdo de itinerancia son redes de UMTS.

Además, para simplificar la descripción e ilustración, se concentra en la diferencia entre un RB convencional y un RB avanzado según la presente realización, es decir no se muestran otros detalles de implementación, sino que se consideran evidentes para un experto.

En un nivel alto, hay una diferencia en un controlador de acuerdo de itinerancia (controlador de RoA) que puede combinar ramas de acuerdo de itinerancia para establecer acuerdos de itinerancia. Además, el controlador de acuerdo de itinerancia hace que se generen reglas de manera que sólo se configura el acuerdo de itinerancia seleccionado.

El intermediario de itinerancia avanzado y el proceso de establecimiento de acuerdo de itinerancia relacionado se describen a continuación en el presente documento en detalle haciendo referencia a la figura 3.

De antemano, la gestión del RB puede configurar políticas en un punto de decisión de políticas (PDP) que rige el proceso de establecimiento de acuerdo de itinerancia (etapa 0).

El sistema de gestión de red (NMS) de PLMN de una PLMN de origen (oPLMN) (etapa 1a) o la gestión de RB (etapa 1b) activa el controlador de acuerdo de itinerancia para establecer un acuerdo de itinerancia entre la oPLMN y (una) PLMN(s) de destino (dPLMN). La activación incluye como información el identificador de la(s) dPLMN(s) con la(s) que debe establecerse el acuerdo de itinerancia individualizado, y si la oPLMN debe volverse una HPLMN o VPLMN o ambas. También podría incluirse información específica de acuerdo de itinerancia adicional tal como una IOT particular o qué servicios están cubiertos por este acuerdo de itinerancia. También es posible incluir varias opciones (por ejemplo un conjunto de servicios n.º 1 y una IOT n.º 1 o un conjunto de servicios n.º 2 y una IOT n.º 2). Esto permite algún grado de flexibilidad al adaptar el acuerdo de itinerancia a un socio particular, abordando así el problema respectivo mencionado anteriormente. Esta etapa puede realizarse mediante señalización o manualmente.

El controlador de acuerdo de itinerancia es un punto de cumplimiento de políticas (PEP). Consulta al PDP si las políticas son aplicables a este par particular de HPLMN y VPLMN(s) y hace que se cumplan estas políticas (etapa 2).

El controlador de acuerdo de itinerancia informa al NMS de la(s) dPLMN(s) del plan de establecer un acuerdo de itinerancia individualizado, pudiendo realizarse esta etapa también manualmente. En este punto, la dPLMN también puede elegir entre opciones (siempre que sean aplicables). El establecimiento de acuerdo de itinerancia procede sólo con esas dPLMN que se confirman (etapa 3).

El controlador de acuerdo de itinerancia extrae las ramas de acuerdo de itinerancia respectivas del repositorio de ramas de acuerdo de itinerancia (etapa 4). En este caso, una “rama” designará un acuerdo de itinerancia abierto de una red particular (con alguna otra red), pudiendo considerarse que un acuerdo de itinerancia “completo” comprende dos de tales ramas. En un sentido físico, puede considerarse que la rama corresponde a una parte de una conectividad entre redes que ya puede estar presente, pero que no está autorizada para su uso sin un acuerdo de itinerancia establecido. Siempre que no haya ningún acuerdo de itinerancia real establecido, la rama está presente sólo virtualmente. Debe observarse que en la técnica anterior, un intermediario de itinerancia comprendía un conjunto predeterminado de tales ramas que se aplicaba con el intermediario de itinerancia. Sin embargo, según la presente realización, se seleccionan dos ramas específicas según un par de redes respectivos de una pluralidad de ramas predefinidas (en un nivel bajo) en el repositorio de ramas de acuerdo de itinerancia.

El controlador de acuerdo de itinerancia establece el acuerdo de itinerancia individualizado combinando las ramas específicas seleccionadas, incluyendo los nombres de oPLMN y dPLMN(s) y posible información adicional que se incluyó en la activación, y considerando las políticas extraídas previamente. Entonces, se almacena el acuerdo de itinerancia. Esto puede realizarse en la base de datos del acuerdo de itinerancia o en otro elemento adecuado (etapa 5).

El controlador de acuerdo de itinerancia informa al NMS respectivo de oPLMN y dPLMN(s) del acuerdo de itinerancia recién establecido. Si los términos y condiciones son aceptables, se confirman la oPLMN y la dPLMN. Ahora se concluye la primera fase del establecimiento de acuerdo de itinerancia, la fase de negociación, (etapa 6).

Naturalmente, si no hay ningún acuse de recibo de ninguna red interesada, no habrá ningún establecimiento de acuerdo de itinerancia en absoluto. Para la recepción de cualquier acuse de recibo de este tipo, puede implementarse una interrupción tras la cual se finaliza el procedimiento (para la red interesada).

Entonces, comienza la segunda fase de establecimiento de acuerdo de itinerancia, la fase de configuración. Con este fin, el controlador de acuerdo de itinerancia informa al generador de reglas del acuerdo de itinerancia recién establecido (etapa 7).

El generador de reglas extrae el acuerdo de itinerancia de la base de datos del acuerdo de itinerancia y hace funcionar todos los parámetros de configuración, reglas de filtro, ajustes de cortafuegos, etc. (etapa 8).

El generador de reglas distribuye la configuración a varios bloques funcionales especializados dentro del RB, los configuradores. Por ejemplo, las reglas para someter a prueba el acuerdo de itinerancia, para facturación, monitorización y compensación se pasan al configurador respectivo responsable de la configuración de las entidades de prueba, facturación, monitorización y gestión de fallos (etapa 9).

El configurador de traducción de direcciones y de filtro de paquetes actualiza el cortafuegos y el filtro de paquetes para el DNS del RB de manera que oPLMN y dPLMN pueden hacer preguntas al DNS uno acerca del otro. Al mismo tiempo, no se contestarán las preguntas de DNS acerca de oPLMN y dPLMN que se originen de otra PLMN W (véase la figura 2), excepto si PLMN X (véase la figura 2) tiene sus propios acuerdos de itinerancia con oPLMN y dPLMN. Debe observarse que se supone en este caso que las propias entradas de DNS ya se han configurado cuando se acordaron las ramas individuales del acuerdo de itinerancia. Además, se actualizan el filtro de paquetes y la traducción de direcciones en el propio RB (etapa 10a).

El configurador de tabla de encaminamiento de IP configura la tabla de encaminamiento de IP del RB de manera que encamine apropiadamente paquetes entre oPLMN y dPLMN (etapa 10b).

El configurador de gestor de configuración de SCCP provoca la gestión de RB para informar a la portadora de SCCP y/o GRX acerca del nuevo acuerdo de itinerancia de manera que puede encaminar y filtrar correctamente el tráfico. Si la portadora de SCCP / GRX proporciona una interfaz para una configuración automática, ésta naturalmente puede usarse. Alternativamente, ya pueden haberse llevado a cabo todas las configuraciones de SCCP cuando se establecieron en primer lugar las ramas individuales del acuerdo de itinerancia (etapa 10c).

Una vez que se han llevado a cabo las configuraciones y las pruebas, respectivamente, del acuerdo de itinerancia, los configuradores individuales devuelven un acuse de recibo al generador de reglas (etapa 11).

Una vez que el generador de reglas recibió todos los acuses de recibo, envía su propio acuse de recibo al controlador de acuerdo de itinerancia (etapa 12).

El controlador de acuerdo de itinerancia informa al NMS de oPLMN y dPLMN que se establece el acuerdo de itinerancia (etapa 13).

Además, podría usarse una ligera modificación del procedimiento descrito anteriormente para actualizar acuerdos de itinerancia existentes. En este caso, todas las etapas se refieren a un acuerdo de itinerancia existente, y en la etapa 5, se actualiza un acuerdo de itinerancia existente en lugar de establecer un acuerdo de itinerancia nuevo.

Además, también puede considerarse la finalización de un acuerdo de itinerancia o bien antes del establecimiento real o bien después del establecimiento real como sólo otra forma de “realizar un acuerdo” y/o actualizar/cambiar un acuerdo existente y, por tanto, debe considerarse como que está incluida en la descripción anterior.

Aunque anteriormente se describe el ejemplo de coubicación, lo siguiente es aplicable a la modificación cuando HRB y VRB no están en coubicación. En este caso, se supone que tienen una relación fiable. En comparación con el proceso descrito anteriormente, los problemas adicionales que van a resolverse son que es necesario que el RB de la oPLMN encuentre el RB de la dPLMN. Puesto que se supone que los intermediarios de itinerancia tienen una relación fiable, se conocerán entre sí. Pueden concebirse una variedad de mecanismos para encontrar el RB de la dPLMN, por ejemplo, el RB de la oPLMN puede comprobar en sí mismo y luego en todos los demás RB si tienen la “rama que falta” del acuerdo de itinerancia, o se usa un mecanismo basado en DNS. Además, las ramas del acuerdo de itinerancia están en un intermediario de itinerancia diferente y la configuración debe realizarse en ambos RB. En este caso, un RB, por ejemplo el RB de la oPLMN, puede encargarse de la tarea de combinar las dos ramas para establecer el acuerdo de itinerancia completo. Este acuerdo de itinerancia se pasa al RB de la dPLMN. Entonces, el proceso procede como antes. Ambos RB generan reglas y configuran el acuerdo de itinerancia.

La estructura interna del RB avanzado y el proceso descrito anteriormente son en principio los mismos, cuando una o ambas PLMN son de una tecnología diferente, por ejemplo WLAN. La diferencia radica en la ausencia de algunos de los configuradores (por ejemplo el gestor de configuración de SCCP) y posibles configuradores adicionales, por ejemplo un configurador para reglas de políticas en un proxy de AAA.

También puede usarse el RB avanzado para adaptar acuerdos de itinerancia individualizados ya existentes, por ejemplo para actualizar la IOT o servicios cubiertos por el acuerdo de itinerancia.

Por tanto, según la primera realización de la presente invención, se consiguen al menos las siguientes ventajas.

Se superan los problemas de acuerdos de itinerancia multilaterales convencionales descritos anteriormente. Los operadores de PLMN que usan acuerdos de itinerancia intermediados por RB recuperan el control sobre con qué PLMN tienen un acuerdo de itinerancia. Los términos y condiciones del acuerdo de itinerancia individualizado pueden adaptarse dinámicamente en cualquier momento. El proceso de establecimiento puede automatizarse en gran medida. Al mismo tiempo, se evitan los inconvenientes de acuerdos de itinerancia bilaterales convencionales. En comparación con los acuerdos de itinerancia bilaterales convencionales, cada PLMN establece sólo una vez un acuerdo de itinerancia (de una rama) con un RB. El RB es el único socio de comunicación para la PLMN, y es necesario que se establezca sólo una relación fiable con el RB. Los intermediarios de itinerancia son responsables de configurar los acuerdos de itinerancia individualizados reales enlazando las ramas individuales de los acuerdos de itinerancia. Además, según la primera realización de la presente invención, la estructura de principio del RB es la misma, independientemente del tipo de red (tal como UMTS, GSM, WLAN, WiMAX,...).

Por tanto, según la primera realización descrita anteriormente, se proporciona un método y un dispositivo aumentados que permiten establecer acuerdos de itinerancia intermediados por un RB. En este caso, la red doméstica y la(s) red(es) visitada(s) están implicadas en la decisión y configuración del acuerdo de itinerancia intermediado por intermediario(s) de itinerancia. El resultado es un acuerdo de itinerancia individualizado que puede ser bilateral o multilateral, es decir entre una HPLM y varias VPLMN o viceversa. Particularmente, el VRB mantiene múltiples acuerdos de itinerancia de “una rama” con redes visitadas W, X, Y, Z (véase la figura 2) y el HRB mantiene la rama doméstica con la red doméstica. Sin embargo, no se establece automáticamente un acuerdo de itinerancia multilateral. En cambio, la red doméstica y la red visitada determinan qué acuerdos de itinerancia bilaterales o multilaterales deben establecerse, intermediados por el/los intermediario(s) de itinerancia. El/los intermediario(s) de itinerancia combina(n) las ramas de acuerdo de itinerancia individuales para establecer un acuerdo de itinerancia completo. También es posible individualizar algunos parámetros del acuerdo de itinerancia en esa fase, por ejemplo IOT o servicios ofrecidos. La figura 2 presenta un posible resultado. La red doméstica tiene un acuerdo de itinerancia bilateral con la red X, con términos y condiciones específicos para la red X, y un acuerdo de itinerancia multilateral, diferente con las redes Y y Z. La red doméstica no tiene un acuerdo de itinerancia con la red W.

Segunda realización

Sin embargo, en cualquier caso, cuando están implicados intermediarios de itinerancia (RB), las redes visitadas son, en gran medida, invisibles para la red doméstica. Es decir, todo el tráfico se redirige a través de proxy por los intermediarios de itinerancia, y la mayoría de las transacciones empresariales (con la posible excepción de facturación) se realizan con los mismos.

Por otro lado, al mismo tiempo el GSMA/los operadores requieren que se proporcione transparencia.

Por consiguiente, existe el problema adicional de acuerdos de itinerancia intermediados por intermediarios de itinerancia de que la red visitada es completa o parcialmente invisible para la red doméstica (y viceversa), puesto que el tráfico de usuario y el tráfico de señalización se redirigen a través de proxy por un RB. Esto conduce a una latencia aumentada y aumenta la posibilidad de errores. Además, los operadores requieren transparencia. Es decir, el operador debe saber cuándo y cómo está tratando con qué otros operadores.

Otro problema es la sobrecarga incurrida en la actualidad con la instalación de acuerdos de itinerancia. Convencionalmente, los acuerdos de itinerancia se establecen manualmente. Se tarda varios meses para que los mismos se activen. Además, también llevan mucho tiempo las actualizaciones de un acuerdo de itinerancia, por ejemplo para añadir un servicio nuevo.

Según la segunda realización de la presente invención, se proporciona un método y dispositivos para que la red doméstica y la red visitada ya no sean invisibles entre sí, y para que el tráfico se intercambie directamente entre las mismas, reduciendo por tanto la latencia y la posibilidad de errores. Al mismo tiempo, se mantienen las ventajas de establecer el acuerdo de itinerancia a través de un RB. Además, el proceso se vuelve automatizado en tal medida que el establecimiento de acuerdo de itinerancia, y las actualizaciones de acuerdos de itinerancia existentes, se realizan rápidamente y de una manera económica.

La idea básica es dividir el establecimiento de acuerdo de itinerancia en una fase de negociación y una fase de realización. La negociación del acuerdo de itinerancia se intermedia por el RB (en relación con la segunda realización a continuación en el presente documento denominado proxy de NICO; NICO: control de interfuncionamiento de red) como siempre. Sin embargo, luego el proxy de NICO se retira del procedimiento y se entrega a las pasarelas de NICO ubicadas tanto en la red doméstica como en la red visitada. Las pasarelas de NICO organizan la fase de realización provocando la configuración local de DNS, pasarelas de seguridad, cortafuegos, etc.

según los requisitos del acuerdo de itinerancia. Como resultado, el proxy de NICO (es decir, el RB) está implicado de manera mínima en el uso real del acuerdo de itinerancia. El tráfico de usuario y el tráfico de señalización se intercambian directamente entre la red visitada y la red doméstica (a través del CRX/IPX). Debe observarse que el término “control de interfuncionamiento de red” se usa para ilustrar la naturaleza de interfuncionamiento de red del procedimiento y se proporciona por tanto por conveniencia de descripción. Sin embargo, además de esta funcionalidad (que es más una configuración que una operación), no se pretende ninguna limitación.

La arquitectura de red resultante se ilustra en la figura 4 por medio del ejemplo de un acuerdo de itinerancia bilateral (línea gruesa resaltada, compárese con la figura 2).

Una implementación de la segunda realización de la presente invención comprende entonces una pasarela de control de interfuncionamiento de red (NICO GW) tanto en la red visitada como en la red doméstica, y un RB aumentado denominado proxy de NICO.

La NICO GW negocia, en representación de su red, el acuerdo de itinerancia con el proxy de NICO basándose en ramas de acuerdo de itinerancia establecidas previamente. Cuando se aprueba el acuerdo de itinerancia, el proxy de NICO activa la NICO GW respectiva en todas las redes que participan en el acuerdo de itinerancia para realizar el acuerdo de itinerancia basándose en información de configuración disponible en el acuerdo de itinerancia. La NICO GW respectiva genera reglas para una configuración y, por consiguiente, provoca la configuración de los elementos de red en su red, por ejemplo DNS y cortafuegos. Algunas configuraciones se aplican a entidades fuera de la red, por ejemplo el sistema de facturación y el proveedor de SCCP.

La figura 5 ilustra la estructura interna de la NICO GW y las etapas implicadas en el establecimiento de acuerdo de itinerancia. La NICO GW está ubicada en una PLMN A. Para una mejor explicación, se supondrá que la PLMN A origina la petición de establecimiento de acuerdo de itinerancia. Además, se supondrá que el proxy de NICO ya ha almacenado las “ramas” de los acuerdos de itinerancia.

Específicamente, la gestión de la NICO GW puede configurar políticas en un punto de decisión de políticas (PDP) que rige el proceso de establecimiento de acuerdo de itinerancia (etapa 0).

El sistema de gestión de red (NMS) de PLMN del proxy de NICO activa el negociador de acuerdo de itinerancia en la NICO GW de PLMN A para que se establezca un acuerdo de itinerancia entre PLMN A como PLMN de origen (oPLMN), y (una) PLMN(s) de destino (dPLMN). La activación incluye como información el identificador de la(s) dPLMN(s) con la(s) que debe establecerse el acuerdo de itinerancia individualizado, y si la PLMN A debe volverse una HPLMN o VPLMN o ambas (etapa 1).

Adicionalmente, también podría incluirse información específica de acuerdo de itinerancia, aunque esta información también podría proceder de un motor de políticas, por ejemplo una IOT (tarifa entre operadores) particular, o qué servicios están cubiertos por este acuerdo de itinerancia. También es posible incluir varias opciones (por ejemplo un conjunto de servicios n.º 1 / IOT n.º 1 o un conjunto de servicios n.º 2 e IOT n.º 2).

El negociador de acuerdo de itinerancia es un punto de cumplimiento de políticas (PEP). Consulta al PDP si las políticas son aplicables a este par particular de HPLMN y VPLMN(s) y hace que se cumplan estas políticas. Las políticas pueden añadir información adicional (véase más arriba). El negociador de acuerdo de itinerancia también puede implicar un ser humano en la decisión (etapa 2). A menos que las políticas o interacción humana den como resultado que se aborte el proceso, se procede a la etapa 3.

El negociador de acuerdo de itinerancia activa el proxy de NICO para establecer un acuerdo de itinerancia. Incluye la información recopilada hasta ahora, es decir identidades de PLMM, IOT, etc. (etapa 3).

El proxy de NICO establece el acuerdo de itinerancia individualizado combinando las ramas, incluyendo los nombres de oPLMN y dPLMN(s) así como posible información adicional que se incluyó en la activación. Para detalles, se hace referencia a la descripción respectiva de la primera realización. Entonces, el proxy de NICO informa al negociador de acuerdo de itinerancia de la NICO GW en PLMN A y a la(s) pasarela(s) de NMS/NICO de la(s) otra(s) PLMN(s) implicada(s) en el acuerdo de itinerancia del acuerdo de itinerancia recién establecido. Si los términos y condiciones son aceptables, se confirman oPLMN y dPLMN (etapa 4). Naturalmente, si no hay ningún acuse de recibo de ninguna red interesada, no habrá ningún establecimiento de acuerdo de itinerancia en absoluto. Para la recepción de cualquier acuse de recibo de este tipo, puede implementarse una interrupción tras la cual se finaliza el procedimiento (para la red interesada).

El negociador de acuerdo de itinerancia se pone en contacto con el control de base de datos de acuerdo de itinerancia para almacenar el acuerdo de itinerancia en la base de datos de acuerdo de itinerancia. Ahora se concluye la primera fase de establecimiento de acuerdo de itinerancia, la fase de negociación, (etapa 5).

Comienza la segunda fase de establecimiento de acuerdo de itinerancia, la fase de realización. Con este fin, el negociador de acuerdo de itinerancia informa al realizador de acuerdo de itinerancia y al generador de reglas

(abreviado como generador de reglas) del acuerdo de itinerancia recién establecido (etapa 6).

El generador de reglas extrae políticas del PDP (etapa 7).

El generador de reglas hace que el control de credenciales y asociación de seguridad establezca una asociación de seguridad entre los operadores (etapa 8).

En el presente ejemplo, el proxy de NICO actúa como tercera parte de confianza que intermedia el intercambio de credenciales. Las credenciales se almacenan en la base de datos de credenciales y asociación de seguridad (etapa 9).

El generador de reglas extrae el acuerdo de itinerancia de la base de datos de acuerdo de itinerancia y hace funcionar todos los parámetros de configuración, entradas de DNS (si son necesarias), ajustes de cortafuegos, etc. También recopila la información que va a enviarse al sistema de facturación y al proveedor de SCCP (etapa 10).

El generador de reglas distribuye las configuraciones a configuradores (etapa 11).

Los configuradores se interconectan con el NMS de modo que se realizan las configuraciones correspondientes. Alternativamente, los configuradores pueden interconectarse directamente con las entidades de red que van a configurarse (etapa 12).

A continuación se describen ejemplos de configuraciones.

Se informa a la portadora de SCCP y/o GRX acerca del nuevo acuerdo de itinerancia de manera que puede encaminar y filtrar correctamente el tráfico. Si la portadora de SCCP/GRX proporciona una interfaz para información automática, ésta naturalmente también puede usarse. También puede concebirse que el proxy de NICO proporcione una interfaz unificada a la portadora de SCCP/GRX.

Se informa del sistema de facturación (posiblemente externo) del nuevo acuerdo de itinerancia. Esto puede suceder a través de interacción humana o a través de una interacción electrónica directamente con el sistema de facturación.

La pasarela de borde y los cortafuegos están configurados, la pasarela de seguridad está configurada con las claves apropiadas, y, a menos que el GRX proporcione un DNS raíz, el DNS de operadores está configurado de manera que puede resolver el DNS de la(s) dPLMN(s).

Una vez que se han llevado a cabo las configuraciones del acuerdo de itinerancia, los configuradores individuales devuelven un acuse de recibo al generador de reglas (etapa 13).

Una vez que el generador de reglas ha recibido todos los acuses de recibo, envía su propio acuse de recibo al NMS de PLMN de acuerdo de itinerancia y el proxy de NICO de que se ha establecido el acuerdo de itinerancia (etapa 14).

Debe señalarse que ante la alternativa de que otra PLMN originase la petición, el proxy de NICO pediría a la NICO GW que participase en el establecimiento del acuerdo de itinerancia.

La figura 6 ilustra la estructura interna de una NICO GW según la segunda realización de la presente invención en mayor detalle. Muestra un bloque de control que incluye todas las funciones de control tal como se describieron anteriormente, y un bloque de comunicación, incluyendo gestores para la comunicación con entidades exteriores. Se muestra explícitamente la comunicación entre entidades exteriores y entidades de comunicación. Se supone que todas las entidades en el bloque de control pueden comunicarse entre sí. Particularmente, los bloques de control se incluyen para las pruebas, la monitorización y la liberación del acuerdo de itinerancia así como para la gestión de fallos.

Debe observarse que la pasarela de NICO puede ser un aparato autónomo así como una funcionalidad implementada, por ejemplo, en NMS.

La figura 7 ilustra la estructura interna del proxy de NICO según el mismo enfoque, en la que la descripción de sus elementos resulta de la descripción anterior en relación con la figura 5.

El proceso y los dispositivos descritos anteriormente no dependen de la tecnología de la red, por ejemplo UMTS o WLAN.

Además, podría usarse una ligera modificación del procedimiento descrito anteriormente para actualizar acuerdos de itinerancia existentes. En este caso, todas las etapas hacen referencia a un acuerdo de itinerancia existente, y en la etapa 4, se actualiza un acuerdo de itinerancia existente en lugar de establecer un acuerdo de itinerancia nuevo.

Además, puede considerarse también la finalización de un acuerdo de itinerancia o bien antes del establecimiento real o bien después del establecimiento real como sólo otra forma de “realizar un acuerdo” y/o actualizar/cambiar un acuerdo existente y, por tanto, debe considerarse como que está incluida en la descripción anterior.

La segunda realización de la presente invención proporciona las siguientes ventajas. Se resuelve el “problema de transparencia” de los acuerdos de itinerancia intermediados. El tráfico de usuario y el tráfico de señalización se intercambian directamente entre la PLMN respectiva, evitando por tanto la latencia y las causas de los errores. Los operadores conocen con qué PLMN están tratando. Al mismo tiempo, la segunda realización de la presente invención mantiene la ventaja de acuerdos de itinerancia intermediados. Es decir, se trata la negociación del acuerdo de itinerancia con el proxy de NICO basándose en ramas de acuerdo de itinerancia establecidas previamente. De esta manera, se reduce la sobrecarga para el establecimiento de acuerdo de itinerancia. El operador de GRX/IPX mantiene un cliente (en este caso, una PLMN) ofreciendo una negociación de acuerdo de itinerancia flexible (automatizada y simplificada) como servicio. Además, se automatiza el proceso entero, eliminando por tanto los costes debido a una configuración manual, y acelerando el proceso de establecimiento. Finalmente, pueden usarse los mismos dispositivos y procedimientos para actualizar los acuerdos de itinerancia existentes.

Modificación de la segunda realización

Aunque anteriormente se describe el caso en el que un proxy de NICO está implicado en el procedimiento de establecimiento/adaptación de acuerdo de itinerancia, la segunda realización también puede implementarse sin el proxy de NICO. En este caso, las pasarelas de NICO se encargan de las tareas respectivas del proxy de NICO, es decir los elementos correspondientes de la pasarela de NICO realizan estas tareas (véase la descripción respectiva del intermediario de itinerancia avanzado según la primera realización). Por tanto, la modificación de la segunda realización permite la negociación automática de acuerdos de itinerancia sin la implicación de un intermediario de itinerancia.

Puede conseguirse una implementación de realizaciones de la presente invención proporcionando un producto de programa informático realizado como medio legible por ordenador que almacena instrucciones según las realizaciones descritas anteriormente.

Por tanto, según las realizaciones preferidas de la presente invención, se describió anteriormente un aparato para demostrar una funcionalidad de intermediario de itinerancia. El aparato comprende un controlador de negociación para negociar un acuerdo de itinerancia entre una red de origen y una red de destino. El aparato comprende demás un generador de reglas que genera reglas según un acuerdo de itinerancia negociado, y una unidad de configuración configurada para implementar ajustes de configuración según reglas respectivas generadas por el generador de reglas.

Lo descrito anteriormente es lo que se considera actualmente como realizaciones preferidas de la presente invención. Sin embargo, tal como resulta evidente para el lector experto, éstas se proporcionan sólo con fines ilustrativos y de ninguna manera se pretende que la presente invención se limite a las mismas. En cambio, se pretende que se incluyan todas las variaciones y modificaciones que caen dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Intermediario de itinerancia,

que está configurado para tener acceso a un repositorio de ramas de acuerdo de itinerancia que comprende una pluralidad de ramas predefinidas, en el que cada rama consiste en un acuerdo de itinerancia abierto de una red particular con alguna otra red, y en el que un acuerdo de itinerancia completo debe comprender dos de tales ramas, y

que está configurado además para establecer un acuerdo de itinerancia entre un par particular de redes de origen y de destino seleccionando dos ramas específicas a partir de la pluralidad de ramas predefinidas en el repositorio de ramas de acuerdo de itinerancia;

comprendiendo el intermediario de itinerancia:

un controlador de negociación para negociar un acuerdo de itinerancia entre una red de origen y una red de destino;

un generador de reglas que genera reglas según un acuerdo de itinerancia negociado; y

una unidad de configuración configurada para implementar ajustes de configuración según reglas respectivas generadas por el generador de reglas, en el que el controlador de negociación está configurado para provocar la combinación de una rama de acuerdo de itinerancia de la red de origen con una rama de acuerdo de itinerancia de la red de destino.

2. Intermediario de itinerancia según la reivindicación 1, en el que

el acuerdo de itinerancia se negocia considerando políticas específicas para al menos una de la red de origen y la red de destino, y

el generador de reglas está configurado para generar las reglas según estas políticas.

3. Intermediario de itinerancia según la reivindicación 2, en el que

la negociación del acuerdo de itinerancia considerando políticas está configurada para que se realice automáticamente por el controlador de negociación que está configurado para consultar al menos si son aplicables las políticas de la red de origen o la red de destino.

4. Intermediario de itinerancia según la reivindicación 3, en el que

el controlador de negociación está configurado para consultar un punto de decisión de políticas en el que las políticas se almacenan previamente mediante al menos una de la red de origen y la red de destino, y en el que

el punto de decisión de políticas está comprendido en el intermediario de itinerancia.

5. Intermediario de itinerancia según la reivindicación 1, que comprende además una funcionalidad de control de interfuncionamiento de red.

6. Intermediario de itinerancia según la reivindicación 5, que comprende además un controlador de asociación de seguridad configurado para establecer una asociación de seguridad entre la red de origen y la red de destino.

7. Intermediario de itinerancia según la reivindicación 4 o la reivindicación 5, en el que

la funcionalidad de control de interfuncionamiento de red está configurada para intercambiar directamente el tráfico de usuario con una funcionalidad de pasarela de otra red.

8. Sistema que comprende:

un intermediario de itinerancia según una cualquiera de las reivindicaciones 5 a 7, configurado para actuar como funcionalidad de control de interfuncionamiento de red de la red de origen; y

un intermediario de itinerancia según una cualquiera de las reivindicaciones 5 a 7, configurado para actuar como funcionalidad de control de interfuncionamiento de red de la red de destino.

9. Sistema según la reivindicación 8, que comprende además un proxy de control de interfuncionamiento de red configurado para combinar una rama de acuerdo de itinerancia de la red de origen con una rama de acuerdo de itinerancia de la red de destino tras una activación respectiva por el controlador de negociación del intermediario de itinerancia según una cualquiera de las reivindicaciones 5 a 7 y configurado para actuar como funcionalidad de pasarela de control de interfuncionamiento de red de la red de origen.

10. Método para operar un intermediario de itinerancia,

estando el intermediario de itinerancia configurado para tener acceso a un repositorio de ramas de acuerdo de itinerancia que comprende una pluralidad de ramas predefinidas, en el que cada rama consiste en un acuerdo de itinerancia abierto de una red particular con alguna otra red, y en el que un acuerdo de itinerancia completo debe comprender dos de tales ramas, y estando configurado además para establecer un acuerdo de itinerancia entre un par particular de redes de origen y de destino seleccionando dos ramas específicas a partir de la pluralidad de ramas predefinidas en el repositorio de ramas de acuerdo de itinerancia;

comprendiendo el método:

negociar un acuerdo de itinerancia entre una red de origen y una red de destino;

y provocar una combinación de una rama de acuerdo de itinerancia de la red de origen con una rama de acuerdo de itinerancia de la red de destino;

generar reglas según un acuerdo de itinerancia negociado;

implementar ajustes de configuración según reglas respectivas generadas; y

11. Método para operar un intermediario de itinerancia según la reivindicación 10, en el que

el acuerdo de itinerancia se negocia considerando políticas específicas para al menos una de la red de origen y la red de destino, y

las reglas se generan según estas políticas.

12. Método para operar un intermediario de itinerancia según la reivindicación 11, en el que

el acuerdo de itinerancia se negocia automáticamente considerando políticas consultando mediante un controlador de negociación al menos si son aplicables las políticas de la red de origen o la red de destino.

13. Método para operar un intermediario de itinerancia según la reivindicación 12, que comprende además

almacenar previamente las políticas mediante al menos una de la red de origen y la red de destino en un punto de decisión de políticas, que se consulta por el controlador de negociación.

14. Método para operar un intermediario de itinerancia según la reivindicación 10, que comprende además

establecer una asociación de seguridad entre la red de origen y la red de destino.

15. Método para operar un intermediario de itinerancia según una cualquiera de las reivindicaciones 10 a 14, en el que

un proxy de control de interfuncionamiento de red se activa para la combinación.

16. Método para operar un intermediario de itinerancia según una cualquiera de las reivindicaciones 10 a 15, que comprende además intercambiar directamente tráfico de usuario entre la red de origen y la red de destino.

17. Producto de programa informático realizado en un medio legible por ordenador, estando el producto de programa informático configurado para proporcionar instrucciones para llevar a cabo un método para operar un intermediario de itinerancia según una cualquiera de las reivindicaciones 10 a 16.

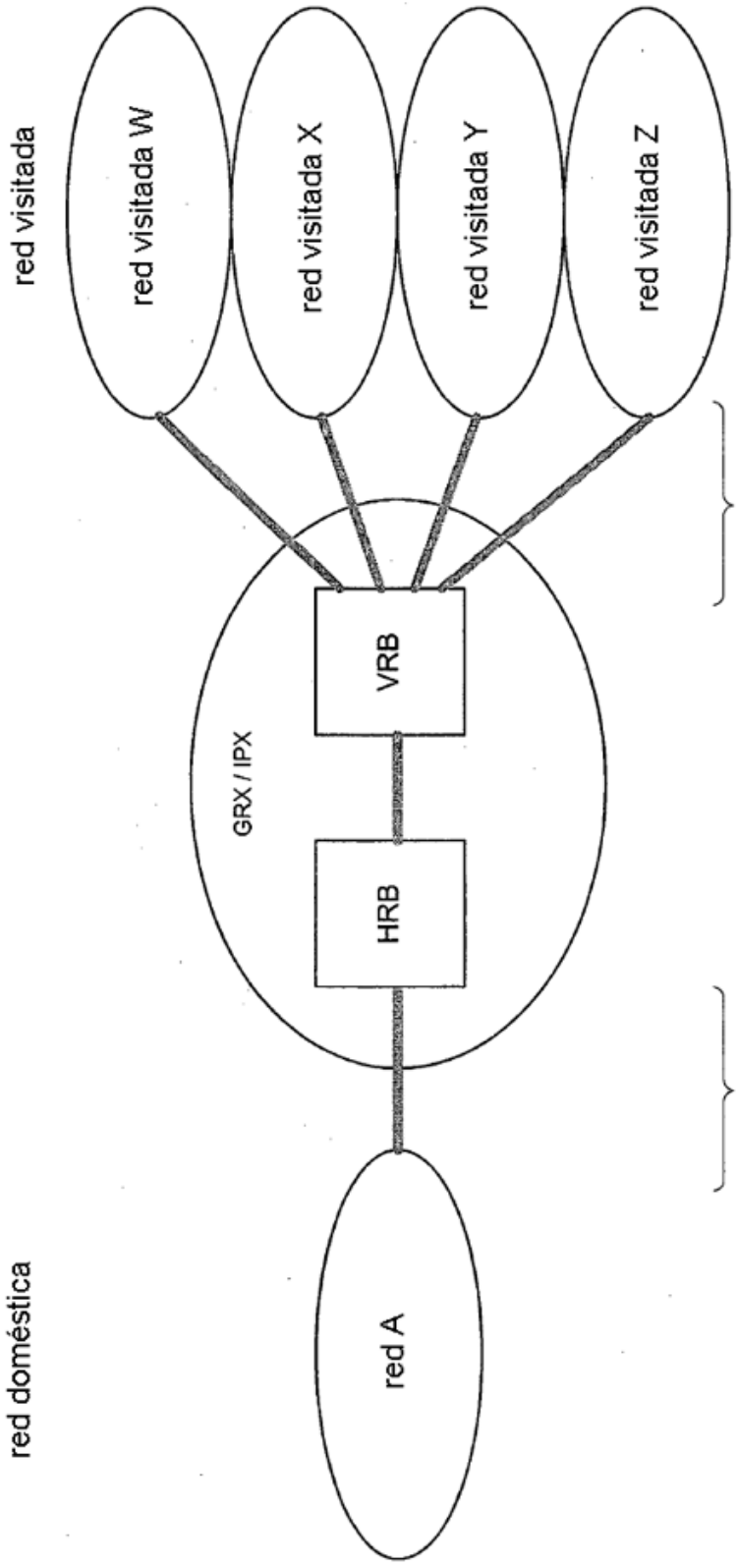

Fig. 1
(Técnica anterior)

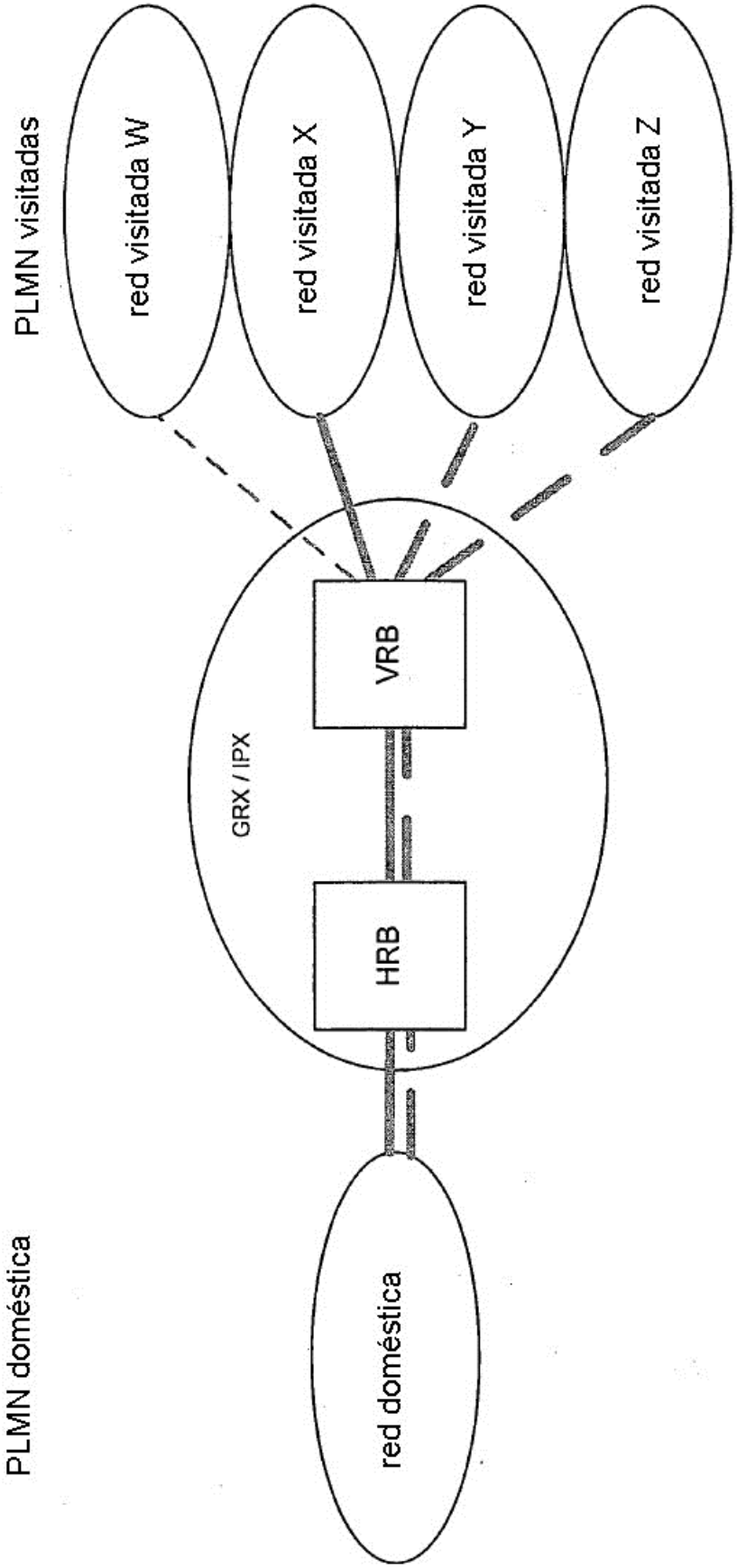
PLMN visitadas
red visitada W
red visitada X
red visitada Y
red visitada Z
GRX / IPX
VRB
HRB
PLMN doméstica
red doméstica

Fig. 2

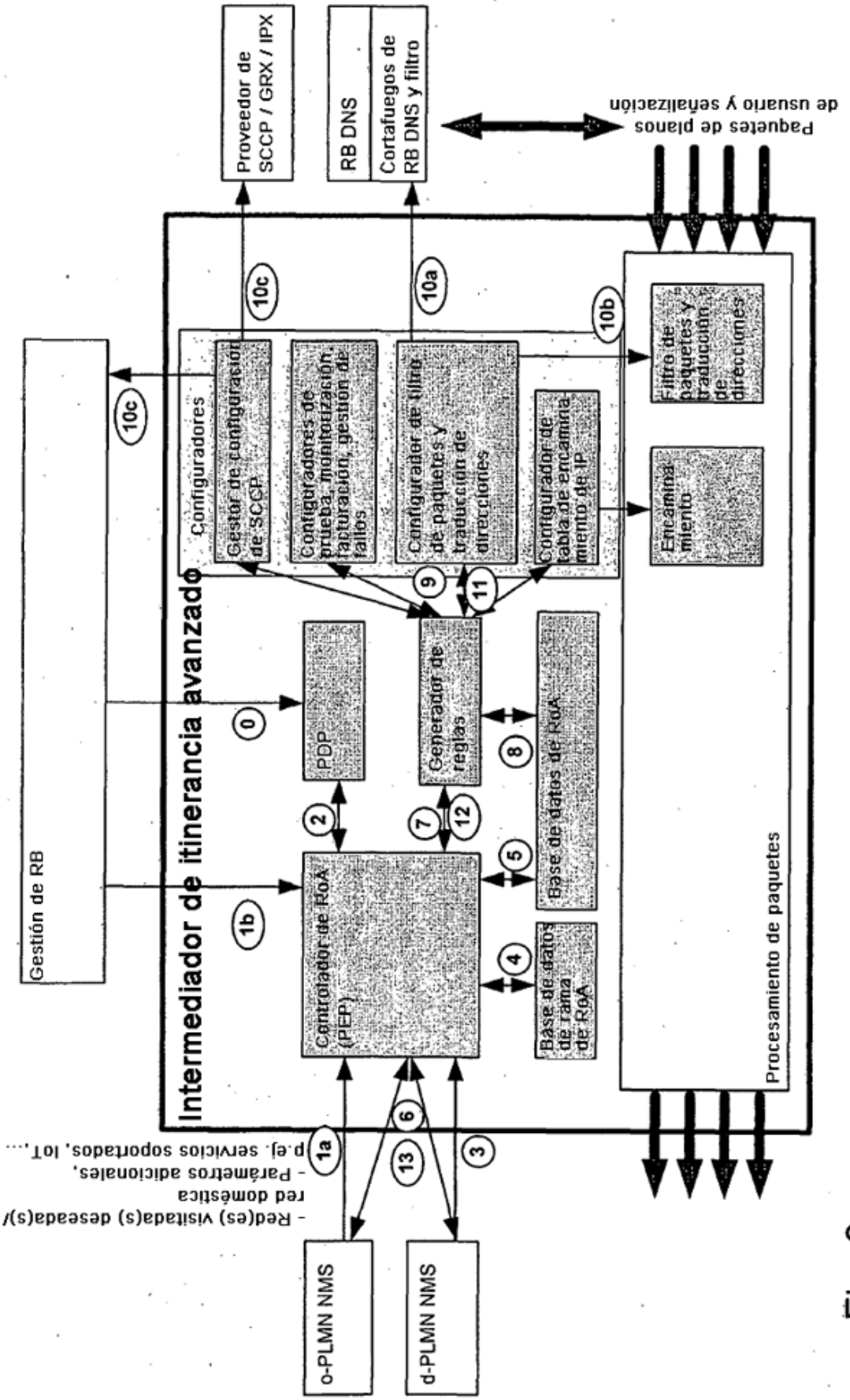
Proveedor de SCCP / GRX / IPX
RB DNS
Cortafuegos de RB DNS y filtro
Paquetes de planos de usuario y señalización
Intermediador de itinerancia avanzado
Configuradores
Gestor de configuración de SCCP
Configuradores de prueba, monitorización, facturación, gestión de fallos
Configurador de filtro de paquetes y traducción de direcciones
Configurador de tabla de encaminamiento de IP
Filtro de paquetes y traducción de direcciones
Encaminamiento
Procesamiento de paquetes
Gestión de RB
PDP
Generador de reglas
Base de datos de RoA
Controlador de RoA (PEP)
Base de datos de rama de RoA
o-PLMN NMS
d-PLMN NMS
- Red(es) visitada(s) deseada(s)/ red doméstica
- Parámetros adicionales, p.ej. servicios soportados, IoT,...
0
1a
1b
2
3
4
5
6
7
8
9
10a
10b
10c
11
12
13

Fig. 3

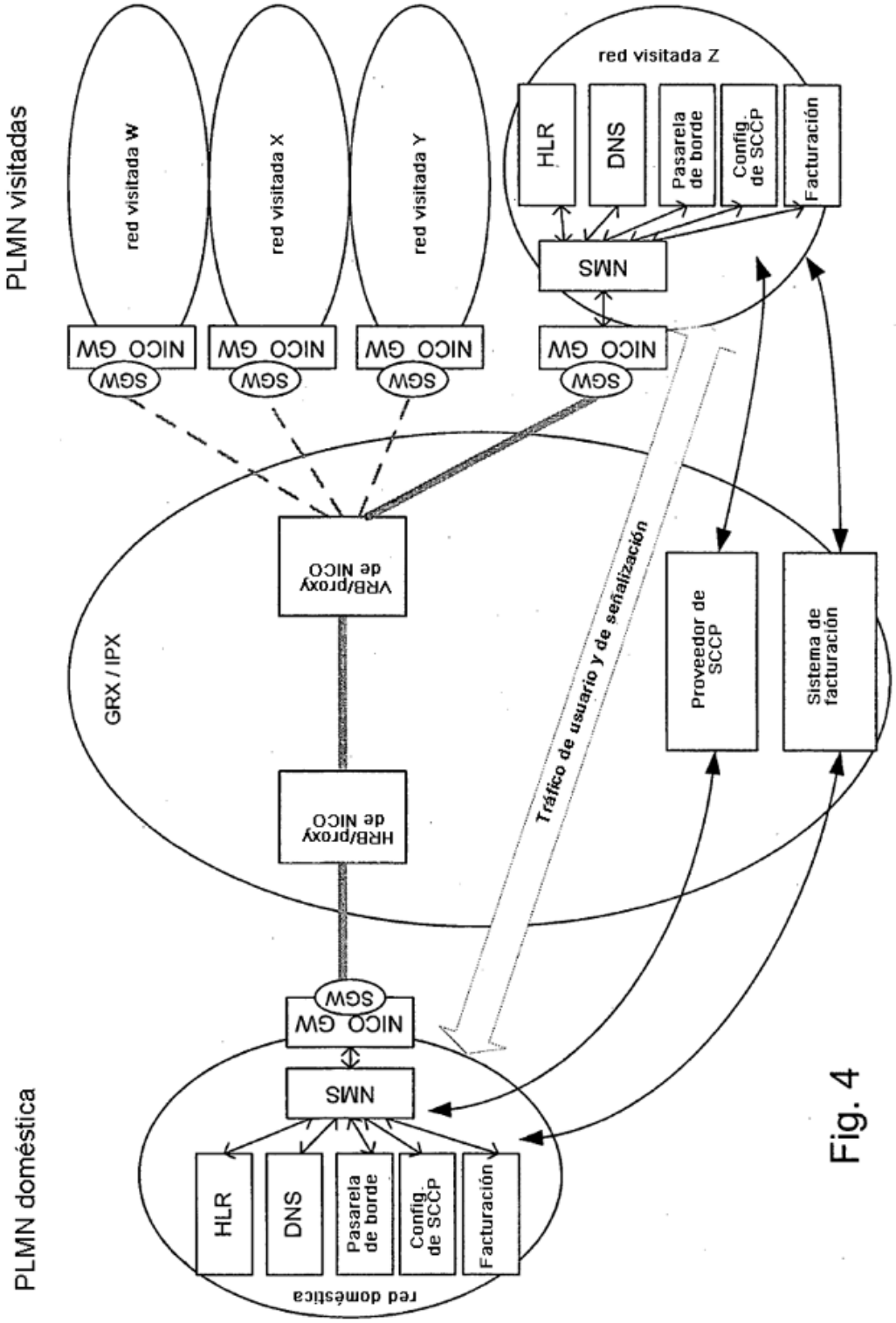
PLMN visitadas
red visitada W
red visitada X
red visitada Y
red visitada Z
HLR
DNS
Pasarela de borde
Config. de SCCP
Facturación
NMS
NICO GW
SGW
VRB/proxy de NICO
GRX / IPX
HRB/proxy de NICO
Tráfico de usuario y de señalización
Proveedor de SCCP
Sistema de facturación
PLMN doméstica
red doméstica

Fig. 4

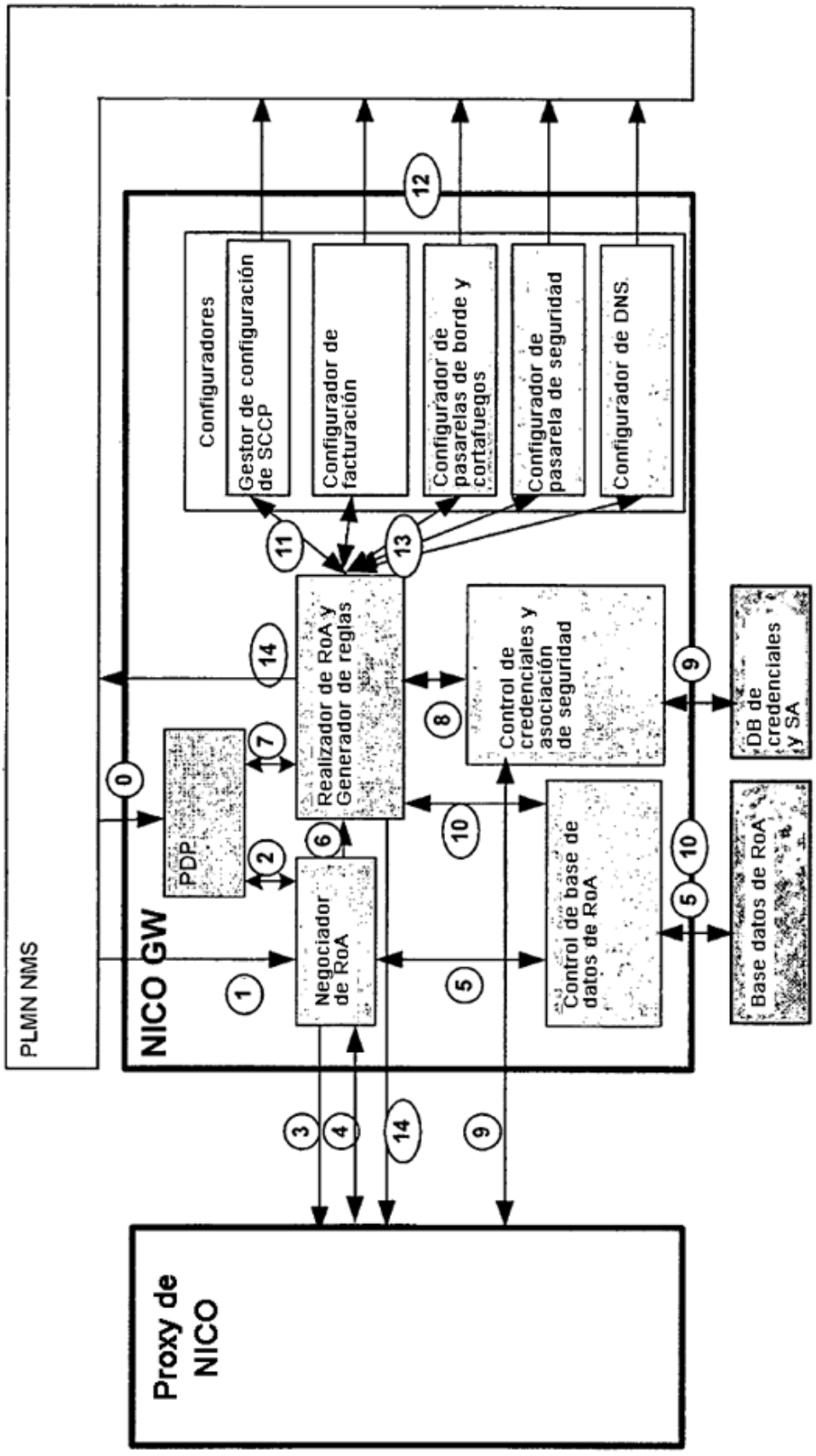
PLMN NMS
NICO GW
Configuradores
Gestor de configuración de SCCP
Configurador de facturación
Configurador de pasarelas de borde y cortafuegos
Configurador de pasarela de seguridad
Configurador de DNS.
PDP
Negociador de RoA
Realizador de RoA y Generador de reglas
Control de credenciales y asociación de seguridad
Control de base de datos de RoA
DB de credenciales y SA
Base datos de RoA
Proxy de NICO
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14

Fig. 5

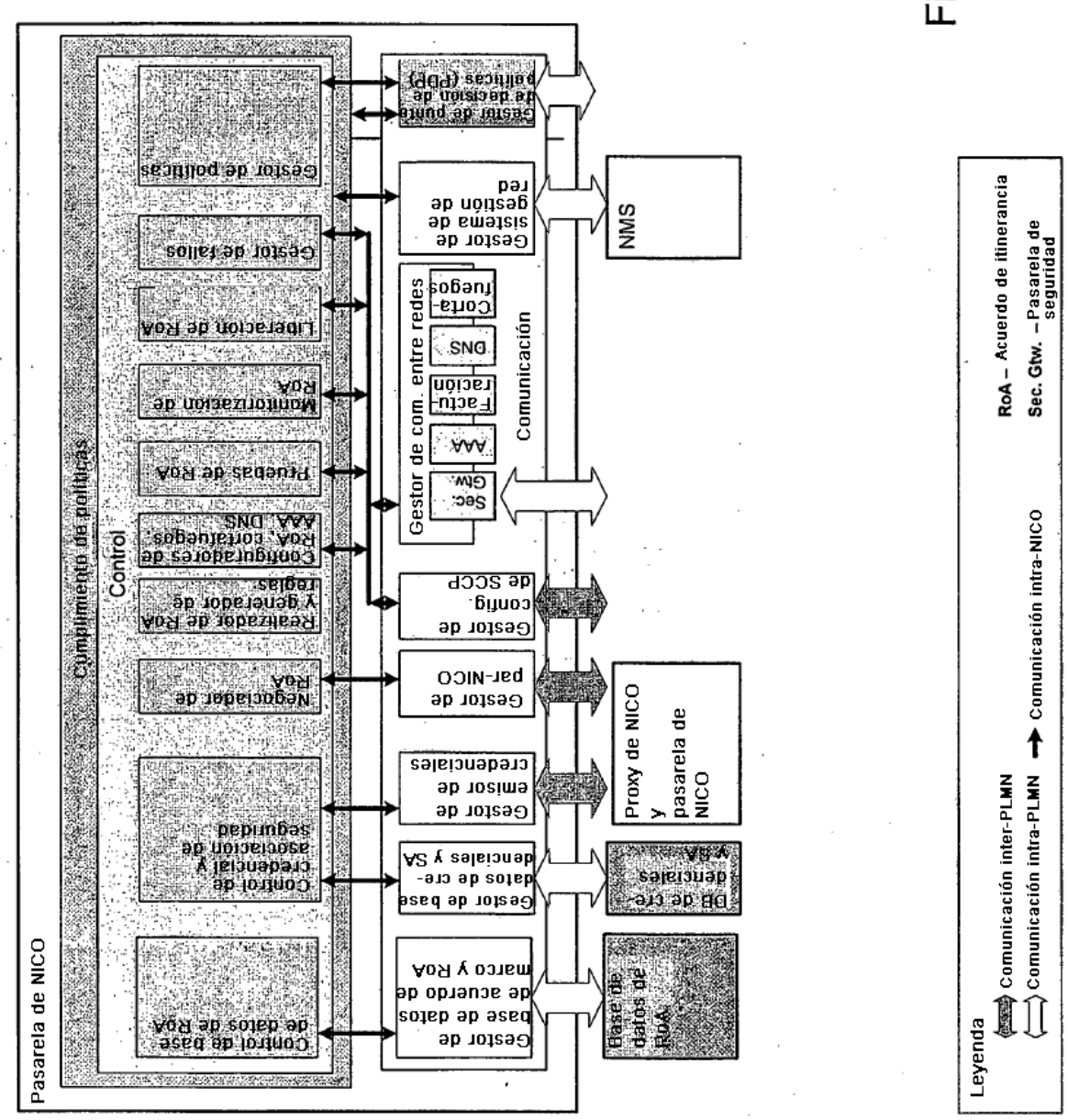
Pasarela de NICO
Cumplimiento de políticas
Control
Control de base de datos de RoA
Control de credencial y asociación de seguridad
Negociador de RoA
Reafirmador de RoA y generador de reglas
Configuradores de RoA, contraseñas, AAA, DNS
Pruebas de RoA
Monitorización de RoA
Liberación de RoA
Gestor de fallos
Gestor de políticas
Gestor de punto de decisión de políticas (PDP)
Gestor de sistema de gestión de red
Gestor de com. entre redes
Sec. Gtw.
AAA
Factu-ración
DNS
Corta-fuegos
Comunicación
Gestor de config. de SCCP
Gestor de par-NICO
Gestor de emisor de credenciales
Gestor de base datos de cre-denciales y SA
Gestor de base de datos de acuerdo de marco y RoA
NMS
Proxy de NICO y pasarela de NICO
DB de cre-denciales y SA
Base de datos de RoA
Leyenda
Comunicación inter-PLMN
Comunicación intra-PLMN
Comunicación intra-NICO
RoA – Acuerdo de itinerancia
Sec. Gtw. – Pasarela de seguridad

Fig. 6

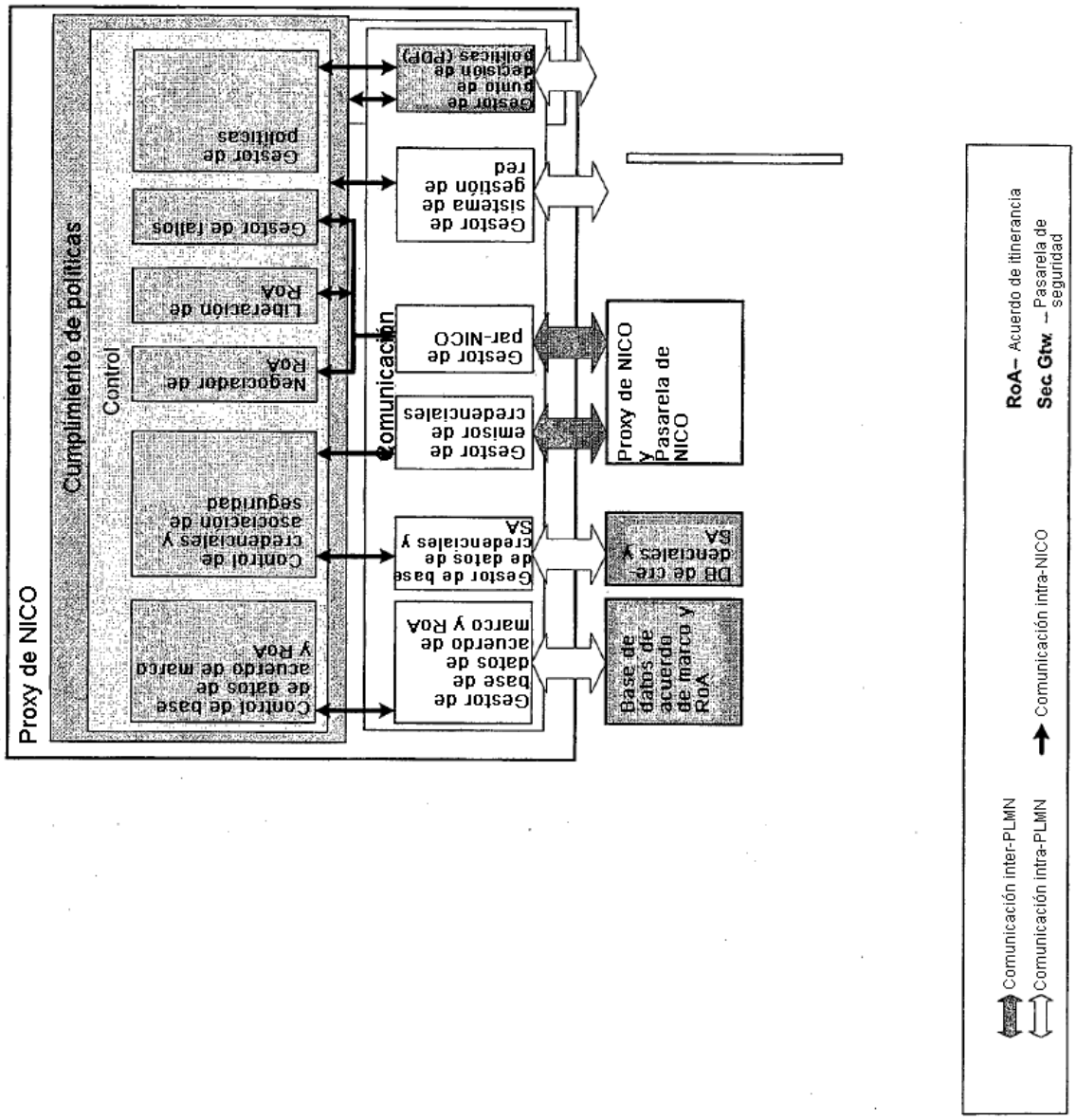
Proxy de NICO
Cumplimiento de políticas
Control
Comunicación
Control de base de datos de acuerdo de marco y RoA
Control de credenciales y asociación de seguridad
Negociador de RoA
Liberación de RoA
Gestor de fallos
Gestor de políticas
Gestor de punto de decisión de políticas (PDP)
Gestor de sistema de gestión de red
Gestor de par-NICO
Gestor de emisor de credenciales
Gestor de base de datos de credenciales y SA
Gestor de base de datos de acuerdo de marco y RoA
Proxy de NICO y Pasarela de NICO
DB de credenciales y SA
Base de datos de acuerdo de marco y RoA
Comunicación inter-PLMN
Comunicación intra-PLMN
Comunicación intra-NICO
RoA– Acuerdo de itinerancia
Sec Gtw. – Pasarela de seguridad

Fig. 7