(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 439 234**

(51) Int. CI.:

H04W 8/08 (2009.01)
H04W 76/04 (2009.01)
H04W 80/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.08.2006 E 06769616 (1)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2013 EP 2052563**

(54) Título: **Proxy de GGSN para una solución de un túnel**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.01.2014

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
PATENT UNIT
164 83 STOCKHOLM, SE

(72) Inventor/es:

RYDNELL, GUNNAR y
RÖNNEKE, HANS BERTIL

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Proxy de GGSN para una solución de un túnel

CAMPO TÉCNICO

La presente invención se refiere al área de la Red de Núcleo de GRPS y a una arquitectura mejorada para proporcionar carga útil de GPRS entre la red de radio y una red de datos en paquetes externa a través de la red de núcleo de PS de GPRS.

ANTECEDENTES DE LA INVENCIÓN

En el 3GPP existe una iniciativa en curso para definir una mejora del GPRS conocida como la Solución de Un Túnel (OTS – One Tunnel Solution, en inglés). El método fue propuesto ya en la Versión 4 del 3GPP y elaborado en el documento TR 23.873 (véase la figura 1a). El TR propone eliminar el plano de usuario de un SGSN (Nodo de Soporte de GPRS de Servicio – Serving GPRS Support Node, en inglés) y enviar carga útil directamente entre el GGSN (Nodo de Soporte de GPRS de Puerta de Enlace – Gateway GPRS Support Node, en inglés) y un RNC (Controlador de Red de Radio – Radio Network Controller, en inglés). El plano de control está todavía implementado en el nodo SGSN, el cual se convierte en un nodo de señalización de control puro sin plano de usuario. No obstante, la propuesta tenía ciertos inconvenientes, por ejemplo, la solución no estaba diseñada para móviles en itinerancia. Para itinerar, el plano de usuario estará conectado a través del SGSN en la red (NW – NetWork, en inglés) visitada hacia el GGSN en la PLMN (Red de Telefonía Móvil Terrestre Pública – Public Land Mobile Network, en inglés) Local, lo que significa que el plano de usuario no puede ser eliminado completamente del SGSN.

Para vencer el problema de la itinerantica, Nortel propuso una arquitectura alternativa, que implicaba el llamado Repetidor de Portador de GGSN en la V-PLMN (véase la figura 1b). Con esta solución el plano de usuario pasará, en caso de itinerancia, a través del GGSN visitado y del RNC, sin pasar a través del SGSN. El SGSN será un nodo de control puro. En la solución del Repetidor de Portador de GGSN, la señalización de control para usuarios en itinerancia será enviada en una interfaz Gp ordinaria entre el V-SGSN y el GGSN Local. Habrá también una interfaz Gn entre el SGSN y el GGSN en la red visitada. Para un usuario en itinerancia estas dos interfaces de control serán utilizadas simultáneamente para señalizar al H-GGSN (GGSN Local – Home-GGSN, en inglés) y al V-GGSN (GGSN Visitado – Visited-GGSN, en inglés).

El Repetidor de Portador de GGSN para la Solución de Un Túnel resuelve algunos, pero no todos, los problemas de la Solución de Un Túnel original en Versión 4.

1. Habrá un problema de seguridad en el Repetidor de Portador de GGSN. Cuando la interfaz Gp se utiliza para usuarios en itinerancia, la topología de la PLMN visitada será abiertamente visible fuera de la V-NW (Red Visitada – Visited-NetWork, en inglés). Los nodos SGSN y sus direcciones de IP están expuestos a las redes GRX y externas además de a los Proxies del GGSN. La señalización de control externa finaliza en varios puntos menos protegidos en el interior de la red, en lugar de en unos pocos puntos bien protegidos en el borde de la NW (Red – NetWork, en inglés).
2. Las configuraciones de cortafuego son complejas cuando el CP (Plano de Control - Control Plane, en inglés) y el UP (Plano de Usuario – User Plane, en inglés) están separados. Los cortafuegos con información de estado no son posibles puesto que la ISRAU (Actualización de Área de Encaminamiento de Inter SGSN – Inter SGSN Routing Area Update, en inglés) será reportada fuera de la V-PLMN.
3. Problema de Itinerancia en la PLMN. Existe un problema en el Repetidor de Portador de GGSN con procedimientos de MM (Gestión de Movilidad – Mobility Management, en inglés) cuando se está itinerando entre diferentes PLMNs. Esto es debido a que el GGSN en la V-PLMN antigua ya no se utilizará, y necesita ser reemplazado con un GGSN en la nueva V-PLMN. 4. Otro problema con la arquitectura de 3GPP de Versión 6 actual es que el tráfico basado en PS (Paquetes Conmutados – Packet Switched, en inglés), por ejemplo, Telefonía sobre IP, está siempre encaminado a la PLMN Local. No hay modo de enviar tráfico localmente en la PLMN Visitada. El Proxy de GGSN proporciona una alternativa para terminar el tráfico de PS en la V-PLMN. Con una implementación específica en el Proxy de GGSN, un Contexto de PDP puede ser forzado a terminar en la V-PLMN. Esto puede, por ejemplo, ser muy importante cuando el dominio de PS deba soportar Telefonía sobre IP de Emergencia, donde el llamante necesita ser conectado a un centro de llamadas de emergencia local en la V-PLMN.

El documento TR 23.809 V0.3.0 (2006-07) del 3GPP de la técnica anterior muestra en 5.3, “GGSN Bearer Relay” que se sugiere un concepto de un túnel en el cual toda la funcionalidad de transporte de plano de usuario es eliminada del SGSN. El nuevo controlador de SGSN (cSGSN) sólo lleva a cabo funciones de control de un SGSN heredado, mientras que el GGSN mejorado (xGGSN) es responsable de la funcionalidad del transporte de plano de usuario de todos los SGSN heredados y del GGSN (véase la Figura 3a). Durante el procedimiento de Activación de Contexto de PDP el cSGSN asigna primero un recurso de plano de portador (TEID y dirección de plano de usuario) del xGGSN. El cSGSN proporciona a continuación el TEID y la dirección del plano de usuario del xGGSN en la solicitud de Crear PDP de Gn. Durante el procedimiento de Establecimiento de RAB el cSGSN pasa el TEID y la dirección del plano de usuario del xGGSN al RNC. Debe observarse que la interacción con el GGSN heredado en

este escenario no requiere ninguna modificación de los procedimientos existentes. En 5.4, se describe un Proxy de GGSN. Este planteamiento es una extensión y mejora del planteamiento de Un Túnel descrito en el TR 23.873 del 3GPP. Este planteamiento es similar al Repetidor de Portador de GGSN de la sub sección 5.3. La diferencia de ese planteamiento es que aquí el xGGSN en lugar del cSGSN realiza la señalización al GGSN de la HPLMN. El SGSN se comunica en la mayoría de los casos con el xGGSN como si fuese el GGSN normal. El xGGSN actualiza a continuación el GGSN de la HPLMN cuando sea necesario. El xGGSN actúa como un SGSN hacia el GGSN de la HPLMN y la interfaz Gp se utiliza entre operadores como en la actualidad. Cuando el cSGSN durante el procedimiento de Activación de Contexto de PDP encuentra un APN que mensaje de Solicitud de Crear Contexto de PDP a ese nodo, por el contrario. El xGGSN crea el Contexto de DPD, asigna los TEIDs adicionales para la interfaz Gp y transmite el mensaje de Solicitud de Crear Contexto de PDP con estos TEIDs al GGSN correspondiente al APN. El mensaje de respuesta del GGSN es devuelto / enviado por el xGGSN al SGSN. En el caso de no itinerancia, el cSGSN podrá descubrir si el GGSN soporta la solución de un túnel o no. Cómo descubrir si el GGSN soporta la solución de un túnel es FFS. Los procedimientos de gestión de movilidad son manejados de la misma manera que cuando la alternativa de Un Túnel es seleccionada en la optimización del portador controlado por el SGSN, no estando el GGSN de la HPLMN implicado en el procedimiento. El xGGSN transmite todas las modificaciones de los Contextos de PDP al GGSN en la HPLMN, a menos que la modificación sea sólo significativa localmente (es decir, que actualice TEIDs y direcciones de IP).

El capítulo 6.18.3 / 5.4 / Figura 4 en el TR 23.809 V0.3.0 (2006-07) del 3GPP – se refiere sólo a un Proxy de GGSN y no se refiere a ninguna itinerancia entre redes VPLMN y no describe ninguna reubicación de proxy, ni describe ninguna señalización para tal itinerancia. Los procedimientos de gestión de movilidad (último párrafo en 5.4) a los que se hace referencia en relación con la Figura 4 parecen referirse a otra forma de movilidad, a saber, transferencia entre redes de radio para la misma VPLMN y siguientes para el mismo Proxy de GGSN. El capítulo 6.18.3 dice “La itinerancia es soportada con el Proxy de GGSN como un repetidor entre el SGSN de la VPLMN y el GGSN de la HPLMN. El Proxy de GGSN actúa como un SGSN hacia el GGSN de la HPLMN y se utiliza la misma interfaz Gp normal”.

COMPENDIO DE LA INVENCIÓN

El objeto de la invención es proporcionar una solución que resuelva al menos algunos de los problemas anteriores.

Este objeto ha sido conseguido mediante el método de acuerdo con la reivindicación 1.

Además, el nodo de soporte de servicio de acuerdo con la reivindicación 6 y el nodo de soporte de puerta de enlace del proxy de la reivindicación 8 también consiguen el objeto anterior.

Se consigue una eficiente reubicación del tráfico de carga útil que es enviado directamente entre una red de radio respectiva de respectivas VPLMNs – entre las cuales está itinerando una unidad de comunicación móvil inalámbrica – hasta un nodo de soporte de puerta de enlace local en una Red de Telefonía Móvil Terrestre Pública Local, HPLMN (Home Public Land Mobile Network, en inglés), a través de respectivos túneles, sin atravesar los nodos de soporte primero y segundo.

Otras ventajas resultarán evidentes a partir de la descripción detallada siguiente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En lo que sigue la invención se describirá de una manera no limitativa con más detalle, con referencia a las realizaciones de ejemplo ilustradas en los dibujos adjuntos, en los cuales:

la Figura 1a y b ilustra esquemáticamente dos realizaciones de soluciones conocidas;
la Figura 2 ilustra esquemáticamente una arquitectura de proxy de GGSN en el contexto de la presente invención;
la Figura 3 ilustra esquemáticamente mejoras de cortafuego con el proxy de GGSN en el contexto de la presente invención;
la Figura 4 ilustra esquemáticamente la itinerancia en la PLMN de acuerdo con una realización de la presente invención;
la Figura 4b ilustra esquemáticamente la itinerancia en la PLMN de acuerdo con otra realización de la presente invención;
la Figura 5 ilustra esquemáticamente la itinerancia regional en el contexto de la presente invención;
la Figura 6 ilustra esquemáticamente un proceso de señalización para itinerancia en la PLMN de acuerdo con una realización de la presente invención;
la Figura 7 ilustra esquemáticamente un proceso de señalización para itinerancia en la PLMN de acuerdo con otra realización de la presente invención;
la Figura 8 ilustra esquemáticamente una red en el contexto de la presente invención; y
la Figura 9 ilustra esquemáticamente un dispositivo de proxy de GGSN de acuerdo con la presente invención.

DESCRIPCIÓN DETALLADA DE REALIZACIONES PREFERIDAS

El concepto básico de esta invención es incluir un Proxy de GGSN en la Solución de Un Túnel (OTS – One Tunnel Solution, en inglés). La diferencia entre la solución del Proxy de GGSN y el Repetidor de Portador de GGSN es que el Proxy de GGSN realiza la señalización a un GGSN de la HPLMN (Nodo de Soporte de GPRS de Puerta en Enlace de Red de Telefonía Móvil Terrestre Pública Local – Home Public Land Mobile Network Gateway GPRS Support Node, en inglés), en lugar de a un SGSN de control. El Proxy de GGSN actúa como un SGSN hacia el GGSN de la HPLMN y por ello una interfaz Gp puede ser preservada entre operadores.

En general, desde el punto de vista de la seguridad la solución de Proxy de GGSN sigue un "principio de Punto de Ahogamiento"; es mejor terminar el tráfico externo en unos pocos puntos bien protegidos en el borde que en muchos puntos menos protegidos del interior de la red. Algunos aspectos relativos a la seguridad del cortafuego para el Proxy de GGSN han sido presentados anteriormente con respecto a la solución de Proxy de GGSN, en la que se sugiere alguna protección en el caso de la PLMN Local. La presente invención es más general y describe también mejoras en la seguridad en el caso de la PLMN Visitada.

El Proxy de GGSN puede ser también un punto posible para envío de emergencia en la PLMN Visitada. En las redes de GGSN actuales el tráfico del dominio de PS para un abonado en itinerancia es siempre encaminado hacia la NW (Red – NetWork, en inglés) local y no hay medio de terminar el tráfico en la red visitada.

La arquitectura de Proxy de GGSN se muestra esquemáticamente en la figura 2, en la que el número de referencia 8 denota una red de acuerdo con la presente invención. Un UE (Equipo de Usuario – User Equipment, en inglés) (no mostrado) se comunica con una red de comunicación de telefonía móvil inalámbrica 8 a través de un controlador 1 de red de radio que a su vez está conectado con la conexión de señalización 2 a un SGSN de control 9, a su vez conectado a un Proxy de GGSN 4 que transmite señales de control a un GGSN de PLMN local 5. Tráfico 3 de carga útil es transportado directamente desde el RNC a la HPLMN a través del Proxy de GGSN 4. El Proxy de GGSN 4 transmite la señalización al GGSN de la HPLMN 5, en lugar de al SGSN de control 9. El Proxy de GGSN 4 actúa como un SGSN hacia el GGSN de la HPLMN 5 y por ello una interfaz Gp puede ser preservada entre operadores.

Cuando el SGSN de control durante el procedimiento de Activación de Contexto de PDP encuentra un APN (Nombre de Punto de Acceso – Access Point Name, en inglés) que pertenece a otra PLMN, selecciona un Proxy de GGSN para manejar el tráfico de itinerancia y envía un mensaje de Solicitud de Crear Contexto de PDP a ese nodo, por el contrario. Un nuevo IE (Elemento de Interfaz, Interface Element, en inglés) con una lista de direcciones de IP al GGSN Local se incluye en la Solicitud de Crear Contexto de PDP. La presencia de este IE es lo que hace que un GGSN sepa que debe actuar como un Proxy de GGSN en lugar de cómo un GGSN.

El Proxy de GGSN crea el Contexto de PDP, asigna TEIDs (Identificador de Punto de Extremo del Túnel – Tunnel End Point IDentifier, en inglés) adicionales para la interfaz Gp y envía el mensaje de Solicitud de Crear Contexto de PDP con estos TEIDs al GGSN correspondiente al APN. El mensaje de respuesta desde el GGSN es devuelto / enviado por el Proxy de GGSN al SGSN.

Los procedimientos de gestión de movilidad son manejados de la misma manera que para la Solución de Un Túnel para tráfico no itinerante, no estando el GGSN de la HPLMN implicado en el procedimiento.

El Proxy de GGSN envía todas las modificaciones de Contextos de PDP al GGSN de la HPLMN, a menos que las modificaciones sólo sean significativas localmente (por ejemplo, actualizar TEIDs y direcciones de IP).

ISRAU y Cortafuegos para Proxy de GGSN

La figura 3 muestra un escenario de Proxy de GGSN y las posibilidades mejoradas para cómo pueden diseñarse cortafuegos en el contexto de la presente invención.

La mejora en este escenario es que el cortafuego sólo ve el Proxy de GGSN. Por ello las transferencias dentro de un operador remoto pueden ser manejadas mediante cortafuegos con información de estado. Las transferencias entre PLMNs raramente están soportadas por los operadores, y pueden ser manejadas específicamente cuando se soportan, por ejemplo, configurando las direcciones de IP de las cuales otros Proxy de GGSNs de operadores pueden enviar en los mensajes de Actualizar Contexto de PDP para alcanzar un túnel de GTP.

Una fabricación de cortafuego puede normalmente no asociar flujos con diferentes direcciones y puertos de IP. El GTP permite el uso de diferentes direcciones y puertos de IP para diferentes mensajes, e incluso el cambio de direcciones de IP sobre la marcha. Utilizar un proxy de GGSN haría más fácil mantener la dirección de IP local a través del cortafuego independientemente de la señalización del SGSN y del GGSN. Un Proxy de GGSN también facilitaría la interoperabilidad del GTP sobre GRX. El soporte de cabeceras en el protocolo GTP puede estar ligado al proxy de GGSN (y no implementado en el cortafuego) lo que haría más fácil el mantener el GTPv1 para tráfico de Gp. Esto es, no hay necesidad de rechazar un GTPv0 debido a cabeceras desconocidas.

Ocultación de topología con proxy de GGSN

La mejora en este escenario es que los SGSNs no necesitan ser expuestos a redes externas. Toda la señalización puede atravesar el Proxy de GGSN y por ello las únicas direcciones de IP que necesitan ser proporcionadas a redes externas son las direcciones de IP del Proxy de GGSN. Este método de acuerdo con la presente invención puede ser también utilizado durante la itinerancia inter PLMN sin exponer ningún SGSN a redes externas, y se ilustra y describe con más detalle a continuación con referencia a la figura 4b.

De acuerdo con esto, esto estaría en línea con el bien conocido “principio de punto de ahogamiento”, es decir, es mejor terminar un tráfico externo inseguro en unos pocos puntos bien protegidos en el borde, que en muchos puntos menos protegidos del interior de la red. El Proxy de GGSN puede ser tal punto bien protegido. Las configuraciones de cortafuegos establecidas en estos pocos puntos pueden ser más eficientes y rentables. El Proxy de GGSN tal como éste es también generalmente menos vulnerable para grandes cantidades de tráfico, por ejemplo, ataques de Denegación de Servicio (DoS – Denial of Service, en inglés), que el SGSN puesto que el GGSN está desde el principio mismo considerado como un nodo de borde y por ello tiene capacidades de mejor rendimiento y mejor filtro, y está diseñado con características de borde.

La interfaz Gp del Proxy de GGSN puede ser entonces conectada a una sub-red separada que está conectada a redes externas, por ejemplo, la red GRX. La dirección de esta sub-red es entonces anunciada por los encaminadores internos al GRX o a otras redes o centrales Inter-PLMN. El Proxy de GGSN puede también ser configurado como un encaminador interno en sí mismo.

Para poder manejar una itinerancia en la PLMN (por ejemplo, utilizando ISRAU, reubicación de SRNS o Transferencia de PS), se propone utilizar un principio ilustrado en las Figuras 4a ó 4b. En la Figura 4a y 4b el número de referencia 401 denota en general un UE y la flecha 416 ilustra cómo se desplaza el UE 401 desde una PLMN a otra PLMN. El UE 401 se comunica con un RNC 402, 407 que a su vez se comunica con un SGSN 403, 408 en cada una de la VPLMN-1 y la VPLMN-2. Los SGSNs se comunican cada uno con un Proxy de GGSN 404, 409 respectivo, el cual a su vez se comunica con un GGSN 405 de la HPLMN del UE 402. Los RNCs pueden estar en contacto 417, 418 con los Proxy de GGSNs 404, 409 en VPLMNs respectivas. En la HPLMN también está situado un HLR 406. La única diferencia entre la alternativa 1 de la figura 4a y la alternativa 2 de la figura 4b es la etapa 1, es decir, cómo son obtenidos los contextos a partir del SGSN antiguo. En la alternativa 1 los dos SGSNs tienen contacto directo 410 (es decir, sobre una red externa, por ejemplo, GRX) y en la alternativa 2 los SGSNs se comunican 419 a través de los Proxies de GGSN 404, 409. En la alternativa 2 la ocultación de topología explicada anteriormente puede ser mantenida, es decir, sólo Proxies de GGSN expuestos a redes externas. Cuando un Proxy de GGSN recibe una Solicitud de Contexto de SGSN utiliza el procedimiento normal traduciendo el RA Antiguo para encontrar el nodo de destino. Con este propósito el Proxy de GGSN tiene una tabla de traducción configurada (RA Antiguo -> dirección de Nodo GSN) para las otras redes con las cuales el operador tiene un acuerdo de itinerancia. Una memoria oculta (caché) puede ser también utilizada para guardar mensajes enviados, pudiendo la memoria oculta ser utilizada cuando los mensajes de respuesta vuelven para saber dónde deben ser enviados. La memoria oculta puede estar presente en el proxy de GGSN antiguo para encontrar el nuevo proxy de GGSN (o SGSN) y en el nuevo proxy de GGSN para encontrar el nuevo SGSN correcto. Por ejemplo el último mensaje que fue enviado puede ser almacenado en la memoria oculta, el cual puede ser eliminado cuando se almacena un nuevo mensaje, cuando el último mensaje ha sido enviado tras una sesión o tras un periodo de expiración.

1. En algún punto del procedimiento MM, los Contextos de PDP son trasladados al nuevo SGSN 408 en la nueva VPLMN. El contenido de estos mensajes no debe cambiar, lo que garantiza la interoperabilidad entre operadores que utilizan Redes de OTS de Versión 7 y operadores que utilizan redes de Versión 6 ó más antiguas. Si el operador utiliza Un Túnel y ha desplegado la seguridad aumentada que el Proxy de GGSN permite, la alternativa 2 anterior se utiliza en lugar de la alternativa 1.
2. Se añade un nuevo mensaje (Solicitud de Reubicar Contexto de PDP) 410 que el SGSN nuevo 408 puede utilizar (si utiliza OTS) para crear un nuevo Contexto de PDP en el Proxy de GGSN 409. Un mensaje de Respuesta de Reubicar Contexto de PDP 411 es devuelto como un reconocimiento por el Proxy de GGSN 409. Si la nueva VPLMN no utiliza OTS sólo usa el procedimiento MM normal (envía un Actualizar Contexto de PDP 412 al GGSN en la HPLMN y continúa hacia la etapa 4 siguiente).
3. El Proxy de GGSN 409 crea el Contexto de PDP pero no envía la creación al GGSN 405, sino que envía un Actualizar Contexto de PDP 412 al GGSN 405, puesto que el Contexto de PDP ya existe en la HPLMN.
4. El nuevo SGSN 408 envía un Actualizar Ubicación 413 al HLR 406, lo cual es reconocido por el HLR 406.
5. Cuando el SGSN antiguo 403 recibe el mensaje de Cancelar Ubicación 414 desde el HLR 406, sabe si el Proxy de GGSN 409 fue utilizado para los Contextos de PDP.
6. Si el SGSN antiguo 403 utilizó un Proxy de GGSN 404 (es decir, utiliza OTS) envía un nuevo mensaje (Solicitud de Borrar Contexto de PDP Reubicado) 415 al Proxy de GGSN 404 en la VPLMN antigua. El Proxy de GGSN antiguo 404 borra a continuación el Contexto de PDP sin enviar nada al GGSN 405 y devuelve un reconocimiento al SGSN antiguo 403 (Respuesta de Borrar Contexto de PDP Reubicado). El SGSN antiguo 403 borra a continuación su Contexto de PDP. Si el SGSN antiguo 403 no utiliza OTS sólo borra su Contexto de PDP (indicado por Cancelar Ubicación). El Cancelar Ubicación del HLR 406 es reconocido.

Este modo de señalización puede funcionar independientemente de si alguna de las VPLMN-1 y VPLMN-2 utiliza OTS o no, e independientemente de si alguna de ellas es una red anterior a la Versión 7. Esto es, no es un requisito que las dos VPLMNs soporten OTS. El reconocimiento funcionará igualmente. Todo depende de lo que haga el SGSN, y para la alternativa 2 también depende de a qué nodos de las tablas de traducción apunta. Un operador, que utiliza OTS y ha empleado la ocultación de topología utilizando Proxies de GGSN, proporciona las direcciones a sus Proxies de GGSN en lugar de a sus SGSNs para sus compañeros de itinerancia (válido para todas las RAs de esta red).

Utilizar el Proxy de GGSN como la única interfaz para otras redes de operadores también puede simplificar el proceso de establecer acuerdos de itinerancia entre operadores. Sólo las direcciones de cada Proxy de GGSN de operador necesitan ser cambiadas. Éstas son válidas para cualquier RAI de la red del otro operador.

La tabla de traducción que se utiliza en un Proxy de GGSN para tener una Ocultación de Topología completa y una configuración de acuerdo de itinerancia simplificada debería ser una tabla de traducción 'bi-direccional'. Los RAIs Antiguos 'Extranjeros' para mensajes salientes serán trasladados a un Proxy de GGSN externo, y para solicitudes entrantes los RAIs a la propia PLMN serán trasladados al SGSN correcto. Lo bueno de esto es que la traducción resulta muy simple si un compañero de itinerancia utiliza Proxy de GGSN. Todos los RAIs de esa PLMN son entonces trasladados a un único Proxy de GGSN externo. Esto facilitará los acuerdos y configuraciones de itinerancia inter PLMN en gran medida y los harán factibles en la práctica. Por razones de redundancia, puede utilizarse más de un Proxy de GGSN si un Proxy de GGSN externo no responde.

Itinerancia regional y Proxy de GGSN

El procedimiento para cambiar el Proxy de GGSN en casos de itinerancia en la PLMN puede ser utilizado para "itinerancia regional", también con una sola PLMN. En redes muy grandes (por ejemplo en China) los operadores pueden encontrar deseable dividir la PLMN en sub-redes menores y aplicar reconocimientos especiales de itinerancia y de optimización del tráfico. La figura 5 que se describe a continuación proporciona algunos ejemplos.

En la etapa 1) de la Figura 4, un UE 500 establece Contextos de PDP a un GGSN en su propia región R/C1. Tanto el "tráfico normal" como cualquier llamada de emergencia puede terminar en este GGSN 506 (línea 501). Mientras está conectado el UE 500 se mueve 504 a otra ciudad / región R/C2 que tiene una configuración de red separada. El SGSN de la nueva región (posiblemente en un nuevo grupo) al cual se conecta el UE identifica que estaba conectado a un SGSN en otra región y a continuación selecciona un Proxy de GGSN para el UE 500. El procedimiento descrito anteriormente con referencia a las Figuras 4a y 4b actualiza el Contexto o los Contextos de PDP para conectarse a través del Proxy de GGSN de la Región 2 al GGSN de la Región 1, como se muestra en la etapa 2) de la figura anterior. Cuando se requiera, puede establecerse también un Contexto de PDP terminado localmente como se muestra en la etapa 2) (línea 502). El Proxy de GGSN de la región 2 puede, por ejemplo, forzar que un Contexto de PDP de emergencia sea establecido localmente, y por ello el Proxy de GGSN en ese caso tomará por el contrario una función de GGSN. Los Contextos de PDP terminados localmente pueden también ser establecidos de otras maneras. Por ejemplo, el establecimiento de un Contexto de PDP terminado localmente puede ser iniciado por el Proxy de GGSN después del reconocimiento de itinerancia en la PLMN (descrito en la figura 4a y 4b). En la etapa 3) el UE se mueve 505 a otra ciudad / región R/C3 más que tiene una configuración de red separada. El reconocimiento descrito para la etapa 2) anterior se repite. Cualquier Contexto de PDP terminado localmente en la etapa 2) es desactivado y reemplazado por un nuevo Contexto de PDP terminado localmente en la región 3 (línea 503).

El diagrama de señalización para la itinerancia en la PLMN mostrada en la Figura 6 es un reconocimiento genérico que puede ser aplicado en reconocimientos de Gestión de Movilidad en general cuando necesita cambiarse el Proxy de GGSN. Esto ocurre normalmente cuando un UE se mueve entre dos PLMNs, pero puede ocurrir también dentro de una sola PLMN, por ejemplo, cuando se utilizan configuraciones de red separadas para diferentes regiones dentro de la PLMN. Para el caso en el que tanto la PLMN nueva como la antigua soporten OTS y se utilice la alternativa 2 (los Proxies de GGSN actúan como nodos intermedios para la Solicitud de Contexto del SGSN - Figura 4b), etapa 1 se envía Nuevo SGSN -> Nuevo Proxy de GGSN -> Antiguo Proxy de GGSN -> Antiguo SGSN y después de vuelta, Antiguo SGSN -> Antiguo Proxy de GGSN -> Nuevo Proxy de GGSN -> Nuevo SGSN. Para el caso en el que sólo la nueva PLMN soporte OTS, etapa 1 se envía Nuevo SGSN -> Nuevo Proxy de GGSN -> Antiguo SGSN y a continuación de vuelta Antiguo SGSN -> Nuevo Proxy de GGSN -> Nuevo SGSN. Y para el caso en el que sólo la PLMN antigua soporte OTS, etapa 1 se envía Nuevo SGSN -> Antiguo Proxy de GGSN -> Antiguo SGSN y a continuación de vuelta Antiguo SGSN -> Antiguo Proxy de GGSN -> Nuevo SGSN. El resto de la señalización es como sigue:

2a. Reubicar Contexto de PDP es enviado desde el nuevo SGSN al nuevo GGSN dentro de la nueva PLMN visitada.

3. Una solicitud de Actualizar Contexto de PDP (TEID del RNC, dirección de IP del RNS, etc.) es enviada desde el nuevo proxy de GGSN al GGSN en la PLMN Local.

3. Una respuesta de actualizar Contexto de PDP es enviada desde el GGSN en la PLMN Local al nuevo proxy de GGSN.
2b. Una respuesta de reubicar Contexto de PDP es enviada desde el nuevo proxy de GGSN al nuevo SGSN.
4a. Un mensaje de actualizar ubicación es enviado desde el nuevo SGSN al HLR.
5a. Un mensaje de cancelar ubicación es enviado desde el HLR al SGSN antiguo en la antigua PLMN visitada.
6. Un mensaje de solicitud de borrar Contexto de PDP reubicado es enviado desde el SGSN antiguo al proxy de GGSN antiguo.
6. Una respuesta de borrar Contexto de PDP reubicado es enviada desde el proxy de GGSN antiguo al SGSN antiguo.
5b. Un mensaje de reconocimiento de cancelar ubicación es enviado desde el SGSN antiguo al HLR.
4b. Un mensaje de reconocimiento de actualizar ubicación es enviado desde el HLR al nuevo SGSN.

La Figura 7 muestra lo que se ve cuando se aplica este reconocimiento genérico en la Actualización de Área de Encaminamiento de Inter SGSN (sub apartado 6.9.1.2.2 en el documento TS 23.060), ISRAU (Inter SGSN Routing Area Update, en inglés). No obstante, debe observarse que la invención también es aplicable a otros procedimientos de movilidad, por ejemplo, pero no estando limitada al procedimiento de reubicación de transferencia de PS, transferencia dura y SNRS (Subsistema de Red de Radio de Servicio – Serving Radio Network Subsystem, en inglés). En la Figura 7 C1, C2 y C3 denotan funciones relativas a CAMEL y son comprendidas por el experto en la materia. El esquema de señalización es como sigue en este ejemplo:

1. Un mensaje de solicitud de actualización de área de encaminamiento es enviado desde el UE al nuevo SGSN a través del BSS.
2. Una solicitud de Contexto de SGSN es enviada desde el nuevo SGSN al antiguo SGSN.
2. El SGSN antiguo envía una respuesta de Contexto de SGSN.
3. Funciones de seguridad son manejadas en este punto.
4. El nuevo SGSN envía un mensaje de reconocimiento de Contexto de SGSN al SGSN antiguo. En esta etapa puede llevarse a cabo C1.
5. El SGSN antiguo envía paquetes.
6a. El nuevo SGSN envía un mensaje de solicitud de reubicación de Contexto de PDP al nuevo proxy de GGSN.
6. El nuevo proxy de GGSN envía una solicitud de actualizar Contexto de PDP al GGSN en la HPLMN.
6. El GGSN de la HPLMN envía una respuesta de actualizar Contexto de PDP.
6b. Una respuesta de reubicar Contexto de PDP es enviada desde el nuevo proxy de GGSN al antiguo SGSN.
7. Un mensaje de actualizar ubicación es enviado desde el nuevo SGSN al HLR de la HPLMN.
8. El HLR envía un mensaje de cancelar ubicación al antiguo SGSN.
8a. El antiguo SGSN envía una solicitud de borrar Contexto de PDP reubicado al antiguo proxy de GGSN.
8b. Una respuesta de borrar contexto de PDP reubicado es enviada desde el proxy de GGSN antiguo al SGSN antiguo.
8. Un mensaje de reconocimiento de cancelar ubicación es enviado desde el SGSN antiguo al HLR.
9. El HLR inserta datos de abonado en el nuevo SGSN.
9. El nuevo SGSN envía un mensaje de reconocimiento de insertar datos de abonado al HLR.
10. El HLR envía un mensaje de reconocimiento de actualizar ubicación al nuevo SGSN. Puede llevarse a cabo C2.
11. El nuevo SGSN envía una aceptación de actualización de área de encaminamiento al UE. Puede llevarse a cabo C3.
12. El UE envía un mensaje de completar actualización de área de encaminamiento al nuevo SGSN.

La Figura 8 ilustra una solución de red general en el contexto de la presente invención con un método de envío local implementado. En la Figura 8 el número de referencia 810 indica de manera general una red de comunicación en la cual opera la presente invención. Un equipo de usuario (UE – User Equipment, en inglés) está comunicado a una red de telefonía móvil pública visitada (VPLMN - Visited Public Land Mobile Network, en inglés) 803 fuera de una red de telefonía móvil terrestre pública local (HPLMN - Home Public Land Mobile Network, en inglés) 804. La presente invención se refiere a una situación en la que el UE visitante 801 se comunica con otro UE 802 y en lugar de comunicarse con la HPLMN 804 del UE visitante 801 estaría interesado en comunicarse directamente a través de la VPLMN 803 con el fin de reducir el encaminamiento de tráfico entre diferentes componentes de la red. La red 810 comprende también enlaces de comunicación 807 entre el UE 801, 802 y el enlace de comunicación 811 de infraestructura entre la VPLMN 803 y la HPLMN 804. La VPLMN 803 y la HPLMN 804 pueden estar conectadas a respectivas redes de comunicación 805 y 806 con respectivos enlaces de comunicación 808 y 809. El tráfico entre el UE visitante 801 y el otro UE 802 es enviado en una ruta de envío local A 808, sin atravesar la PLMN Local 804.

El UE 1 tiene un software SW que es capaz de contar volúmenes de tráfico que pasan a través de él, con una precisión y granularidad arbitrarias, y en algún punto de activación, con la ayuda de un SIM (Módulo de Identidad de Abonado – Subscriber Identity Module, en inglés) 817 asociado al UE 801, generar una firma digital codificada,

"FIRMA" con la información de conteo del tráfico, que es enviada 812 junto con el informe del tráfico, es decir, por ejemplo a la VPLMN 803 ó directamente a la HPLMN 804.

La red visitada 803 tiene la capacidad de coger el nuevo elemento de información, el informe del tráfico y la 'FIRMA', e insertarlo en el siguiente CDR 815 producido 813 por la VPLMN 803 que es enviada 814 para el UE 1 al Operador Local, por ejemplo a un sistema de facturación de un Operador Local 816 ó a un agente de facturación que actúa como bróker de comunicación intermedio.

El sistema de facturación del Operador Local 816 puede descifrar el informe del tráfico de información y la "FIRMA" y utilizarlo para validar la corrección de los bytes contados que la Red Visitada y el equipo de usuario 801 han reportado. El método de envío local y las implementaciones con respecto a la ocultación de topología han sido explicados en otra solicitud de patente con número de publicación WO 2008/003344.

Volviendo ahora a la Figura 9, que ilustra en un diagrama esquemático un nodo de infraestructura (proxy de GGSN o SGSN) de acuerdo con la presente invención (por ejemplo un nodo de soporte), en el que una unidad de procesamiento 901 maneja datos de comunicación e información de control de comunicación. El nodo de infraestructura 900 comprende también una memoria volátil (por ejemplo RAM) 902 y/o una memoria no volátil (por ejemplo, un disco duro o un disco rápido) 903, y una unidad de interfaz 904. El nodo de infraestructura 900 puede comprender también una unidad de comunicación de aguas abajo 905 y una unidad de comunicación de aguas arriba 906, cada una con una interfaz de conexión respectiva. Todas las unidades del nodo de infraestructura pueden comunicarse entre sí directa o indirectamente a través de la unidad de procesamiento 901. El software para manejar la comunicación hacia y desde las unidades de telefonía móvil unidas a la red es al menos parcialmente ejecutado en este nodo y puede ser almacenado también en el nodo; no obstante, el software puede ser también cargado dinámicamente durante el inicio del nodo o en una etapa posterior durante, por ejemplo, un intervalo de servicio. El software puede ser implementado como un producto de programa de ordenador y distribuido y/o almacenado en unos medios legibles por ordenador extraíbles, por ejemplo disquete, CD (Disco Compacto – Compact Disc, en inglés), DVD (Disco de Video Digital – Digital Video Disk, en inglés), medios de memoria rápida o similar extraíbles (por ejemplo, medios de memoria extraíbles basados en memoria rápida compacta, memoria digital segura SD (Secure Digital, en inglés), pincho de memoria, miniSD, tarjeta de multimedios MMC (MultiMedia Card, en inglés), smartmedia, transflash, XC) , HD-DVD (DVD de Alta Definición – High Definition, en inglés), un DVD de Bluray, USB (Bus de Serie Universal – Universal Serial Bus, en inglés), medios de cinta magnética, medios de almacenamiento óptico, medios magneto-ópticos, memoria de burbuja o distribuidos como una señal propagada a través de una red (por ejemplo, Ethernet, ATM, ISDN PSTN, X.25, Internet, Red de Área Local (LAN – Local Área Network, en inglés), o redes similares capaces de transportar paquetes de datos al nodo de Proxy de GGSN).

Ventajas de la presente invención

Beneficios con el Proxy de GGSN en comparación con el Repetidor de Portador de GGSN y en comparación con la Versión 6 del 3GPP actual:

1. El Proxy de GGSN puede simplificar la itinerancia en la PLMN. Con la itinerancia de alternativa 2, sólo se requiere que una única dirección de IP (para un Proxy de GGSN) sea cambiada para permitir la itinerancia entre dos PLMNs. Las direcciones de IP actuales para todos o un intervalo de RAs necesitan ser cambiadas en un acuerdo de itinerancia de PLMN. Esto puede reducir costes para los acuerdos de itinerancia de los operadores significativamente. Por supuesto las direcciones de IP de dos o más Proxies de GGSN pueden ser cambiadas por razones de redundancia o de capacidad. ¡Con procedimientos de itinerancia de PLMN simplificados, la itinerancia den la PLMN puede ser una realidad en la práctica!
2. Mayor seguridad en la red de núcleo. La ocultación de topología permite que la red troncal CN (redes de GN y Iu) sea aislada del GRX y de otras redes externas. Con interfaces de GP separadas en el SGSN el aislamiento de GP ha sido posible ya antes, pero ahora ningún SGSN en absoluto necesita ser abierto a la externalidad. Sólo uno o unos pocos Proxies de GGSN pueden estar situados en el interior entre la PLMN y las redes externas. Esto simplifica significativamente el diseño de la red. La topología de la CN está también completamente oculta al exterior. Ningún SGSN o RNC será alcanzable o conocido desde el exterior de la PLMN.
3. La ocultación de topología y el simple diseño de red utilizando Proxies de GGSN en el interior puede también simplificar otras necesidades específicas que tiene un operador. Por ejemplo, el uso de direcciones de IP privadas en la CN, y facilita la migración a IPv6. La colocación de los puntos de traducción de dirección de IPv4 a IPv6 (NAT-PTs) puede ser facilitada mediante un diseño de red más simple en el interior. El Proxy de GGSN puede incluso ser utilizado como un traductor de protocolo (NAT-PT).
4. Utilizar la solución de proxy de GGSN puede hacer los acuerdos de itinerancia Inter PLMN entre operadores más fáciles de establecer, lo que creará la posibilidad de mantener la aplicación de PS, por ejemplo, VoIP, operativa durante la itinerancia entre PLMNs. Es necesario intercambiar menos información utilizando la solución de proxy de GGSN, en comparación con la actual solución. Es suficiente con configurar en el proxy de GGSN la dirección al proxy de GGSN de los operadores que cooperan, y por lo tanto no es necesario configurar todas las direcciones de SGSN para todas las demás RAs de los operadores.

5. Con el Proxy de GGSN ciertas características de la red pueden ser concentradas en el GGSN (carga, control de política, LI) y pueden entonces aplicar a todo el tráfico independientemente de si es tráfico itinerante o no itinerante. Esto permite mejores características y simplifica las configuraciones de la red. Hoy en día se requiere aún que un operador que ha desplegado funciones de carga en el GGSN mantenga funciones de carga en el SGSN para el tráfico visitante. Y no es posible desplegar el control de política para el tráfico itinerante (visitante) con los estándares de hoy en día.

6. Tráfico de plano de usuario optimizado, lo que puede ahorrar costes de transporte. El tráfico nunca tiene que ser encaminado a través del GGSN y siempre puede tomar la ruta más corta entre el RNC y el GGSN.

7. El tráfico de plano de usuario es encaminado en rutas predecibles en la CN. Con el plano de usuario completamente eliminado del SGSN, el tráfico del plano de usuario siempre estará encaminado a lo largo de algunas rutas en la CN independientemente de si el tráfico es itinerante, se realiza LI, etc. Esto debería simplificar el diseño de la red y facilitar el uso de diferentes 'sondas' en la red (para carga, monitorización del tráfico, diferentes proxies, etc).

8. Permite envío local de tráfico de emergencia. Para tráfico itinerante, el Proxy de GGSN es un punto natural para terminar los Contextos de PDP específicos que por ejemplo pueden ser utilizados para conectar la telefonía sobre IP de emergencia a centros de emergencias locales.

9. Ningún tráfico de plano de usuario del SGSN de 3G puede permitir productos de SGSN simplificados más rentables. El hardware de plano de usuario restante en los SGSNs de 2G / 3G de acceso dual existentes puede ser utilizado para manejar más tráfico de 2G.

10. CP y UP no están separados (en comparación con el Repetidor de Portador de GGSN alternativo). Esto puede hacer las configuraciones del cortafuego menos complejas. El manejo del error puede también hacerse más simple (tanto CP como UP en el mismo nodo). Por ejemplo el reinicio del nodo resulta menos complejo – no hay estados distribuidos como en la propuesta del Repetidor de Portador de GGSN.

El término itinerancia como ha sido utilizado en este contexto se define como la capacidad de que un cliente de telefonía móvil haga y reciba automáticamente llamadas de voz, envíe y reciba datos, o acceda a otros servicios cuando viaja fuera del área de cobertura geográfica en la red local, a través de una red visitada; la red visitada puede pertenecer al operador al cual pertenece el cliente o puede pertenecer a un operador externo. La itinerancia es técnicamente soportada por procedimientos de gestión de movilidad y, por procedimientos de autenticación, autorización y registro de operaciones. El establecimiento de la itinerancia entre operadores de red se basa en acuerdos de itinerancia entre operadores directa o indirectamente a través de brókers o agentes de itinerancia. Si la red visitada está en el mismo país que la red local, esto se conoce como itinerancia internacional.

Los problemas de facturación y tarificación son tratados en relación con la presente invención de acuerdo con procedimientos estándar por ejemplo a través de un protocolo de AAA (Autenticación, Autorización y Registro de Operaciones – Authentication, Authorization and Accounting, en inglés) entre entidades de las redes, por ejemplo, a través de un protocolo como RADIUS (Marcado de Autenticación Remota en Servicio de Usuario – Remote Authentication Dial in User Service, en inglés) o Diameter. No obstante, con el método de envío local habilitado también el UE está implicado en el conteo del tráfico y estos datos son reportados junto con los datos de conteo del tráfico de la red visitada a la PLMN local como se ha descrito anteriormente en este documento.

Debe observarse que la palabra "comprende" no excluye la presencia de otros elementos o etapas distintos de los listados. La invención puede al menos en parte ser implementada en software o hardware. Debe observarse también que cualquier signo de referencia no limita el alcance de las reivindicaciones, y que varios "medios", "dispositivos" y "unidades" pueden ser representados por el mismo elemento de hardware.

Las realizaciones mencionadas y descritas anteriormente están dadas sólo como ejemplos y no deben ser consideradas como limitativas de la presente invención, la cual puede abarcar otras realizaciones dentro del alcance de la invención de acuerdo con las reivindicaciones de la patente que se describen a continuación.

DEFINICIONES

GTP	Protocolo de Tunelización	GPRS Tunneling Protocol, en inglés
GRX	Central de Itinerancia de GPRS	GPRS Roaming eXchange, en inglés (inter PLMN network provided by Specific network providers for international GPRS traffic)
IE	Elemento de Información	Information Element, en inglés ("protocol parameter")
LI	Interceptación Legal	Lawful Intercept, en inglés
NAT-PT	Traducción de Dirección de Red – Protocolo de Traducción	Network Address Translation – Protocol Translation, en inglés
NW	Red	NetWork, en inglés
OTS	Solución de Un Túnel	One Tunnel Solution, en inglés
PDN	Red de Datos en Paquetes	Packet Data Network, en inglés
PDP	Protocolo de Datos en Paquetes	Packet Data Protocol, en inglés
PDP_Context	Un túnel establecido entre un terminal y un GGSN en una red del 3GPP	

El túnel es, por ejemplo utilizado para tunelizar paquetes de IP entre el UE e Internet y o redes de servicio

proporcionadas por el operador.

El término Contexto de PDP es en algunos contextos también utilizado para el conjunto de parámetros utilizados para gestionar un contexto de PDP en un nodo (por ejemplo, un SGSN o GGSN.

PLMN	Red de Telefonía Móvil Terrestre Pública	Public Land Mobile Network, en inglés
HPLMN	PLMN Local	Home PLMN, en inglés (la red local para un abonado)
VPLMN	PLMN Visitada (la red que visita un abonado)	Visited PLMN, en inglés
RA	Área de Encaminamiento	Routing Area, en inglés
RAU	Actualización de Área de Encaminamiento	Routing Area Update, en inglés
TEID	Identificador de Punto de Extremo de Túnel	Tunnel Endpoint IDentifier, en inglés
UE	Equipo de Usuario	User Equipment, en inglés

REIVINDICACIONES

1. Un método para itinerancia de una unidad de comunicación de telefonía móvil inalámbrica (401) desde una primera Red de Telefonía Móvil Terrestre Pública visitada, VPLMN, (VPLMN1) a una segunda VPLMN (VPLMN2), comprendiendo la primera VPLMN un primer nodo de soporte de servicio (403) y un primer nodo de soporte de puerta de enlace de proxy (404); comprendiendo la segunda VPLMN un segundo nodo de soporte de servicio (408) y un segundo nodo de soporte de puerta de enlace de proxy (409), en el que la carga útil es enviada directamente entre una red de radio respectiva de la VPLMN respectiva a un nodo de soporte de puerta de enlace local (405) en una Red de Telefonía Móvil Terrestre Pública Local, HPLMN, a través de respectivos túneles (417, 418), sin atravesar los nodos de soporte de servicio primero y segundo,
comprendiendo el método las etapas de:

a. enviar una solicitud de contexto desde el segundo nodo de soporte de servicio (408) en la segunda VPLMN al primer nodo de soporte de servicio (403) en la primera VPLMN;
b. recibir una respuesta de contexto en el segundo nodo de soporte de servicio desde el primer nodo de soporte de servicio;
c. enviar un reconocimiento de contexto desde el segundo nodo de soporte de servicio al primer nodo de soporte de servicio;
d. enviar una solicitud de reubicar contexto de Protocolo de Datos en Paquetes, es decir, PDP (Packet Data Protocol, en inglés), desde el segundo nodo de soporte de servicio al segundo nodo de soporte de puerta de enlace de proxy (409) en la segunda VPLMN;
e. enviar una solicitud de actualizar contexto de PDP al nodo de soporte de puerta de enlace local (405) en la HPLMN de la unidad de comunicación de telefonía móvil inalámbrica desde el segundo nodo de soporte de puerta de enlace de proxy;
f. recibir en el segundo nodo de soporte de puerta de enlace de proxy una respuesta de actualizar contexto de PDP;
g. enviar una respuesta de reubicar contexto de PDP al segundo nodo de soporte de servicio desde el segundo nodo de soporte de puerta de enlace de proxy;
h. enviar un mensaje de actualizar ubicación desde el segundo nodo de soporte de servicio a un registro de ubicación local (406) en la HPLMN de la unidad de comunicación de telefonía móvil inalámbrica (401);
i. recibir un mensaje de reconocimiento de actualizar ubicación en el segundo nodo de soporte de servicio desde el registro de ubicación local.

2. El método de acuerdo con la reivindicación 1, en el que el segundo nodo de soporte de puerta de enlace de proxy (409) actúa como un nodo intermedio para toda la comunicación de control en las etapas a a c, es decir, que la solicitud de contexto, respuesta de contexto y reconocimiento de contexto son transmitidas a través del segundo nodo de soporte de puerta de enlace de proxy (409).

3. El método de acuerdo con la reivindicación 1, en el que un primer nodo de soporte de puerta de enlace de proxy (404) situado en la primera VPLMN actúa como un nodo intermedio para toda la comunicación de control en las etapas a a c, esto es, que la solicitud de contexto, la respuesta de contexto y el reconocimiento de contexto son transmitidos a través del primer nodo de soporte de puerta de enlace de proxy (404).

4. El método de acuerdo con la reivindicación 1, que comprende también las etapas de:

j. recibir un mensaje de cancelar ubicación desde el registro de ubicación local en la PLMN Local de la unidad de comunicación de telefonía mocil inalámbrica;
k. enviar una solicitud de borrar contexto de Protocolo de Datos en Paquetes, es decir, PDP (Packet Data Protocol, en inglés) reubicado desde el primer nodo de soporte de servicio a un primer nodo de soporte de puerta de enlace de proxy (404) en la primera VPLMN;
l. enviar una repuesta de borrar contexto de PDP reubicado al primer nodo de soporte de servicio desde el primer nodo de soporte de puerta de enlace de proxy; y
m. enviar un mensaje de reconocimiento de cancelar ubicación al registro de ubicación local.

5. El método de acuerdo con la reivindicación 1, que comprende también las etapas de

- recibir información de conteo de tráfico desde la unidad de comunicación de telefonía móvil inalámbrica en los nodos de soporte de servicio primero y segundo (403, 408);
- combinar información de conteo de tráfico desde el equipo de usuario con información de conteo de tráfico desde los nodos de soporte de servicio en un mensaje de tarificación; y
- enviar el mensaje de tarificación a un servidor de facturación local.

6. Un nodo de soporte de servicio (408), para permitir que una unidad de comunicación de telefonía móvil inalámbrica (401) itinere desde una primera Red de Telefonía Móvil Terrestre Pública visitada, VPLMN (Visited Public Land Mobile Network, en inglés), (VPLMN1) a una segunda VPLMN, (VPLMN 2), comprendiendo la primera

VPLMN un primer nodo de soporte de servicio (403) y un primer nodo de soporte de puerta de enlace de proxy (404); comprendiendo la segunda VPLMN el nodo de soporte de servicio (408), constituyendo un segundo nodo de soporte de servicio, y un segundo nodo de soporte de puerta de enlace de proxy (409), en el que se envía carga útil directamente entre una red de radio respectiva de la VPLMN respectiva a un nodo de soporte de puerta de enlace local (405) en una Red de Telefonía Móvil Terrestre Pública Local, HPLMN (Home Public Land Mobile Network, en inglés), HPLMN, a través de respectivos túneles, sin atravesar los nodos de soporte primero y segundo, comprendiendo el nodo de soporte de servicio (408) una unidad de procesamiento (901) que está adaptada para:

a. enviar una solicitud de contexto al primer nodo de soporte de servicio (403) en la primera VPLMN para la unidad de comunicación de telefonía móvil inalámbrica (401);
b. recibir una respuesta de contexto desde el primer nodo de soporte de servicio;
c. enviar un reconocimiento de contexto al primer nodo de soporte de servicio;
d. enviar una solicitud de reubicar contexto de PDP al segundo nodo de soporte de puerta de enlace de proxy (409) en la PLMN actual;
e. recibir una respuesta de reubicar contexto de PDP desde el segundo nodo de soporte de puerta de enlace de proxy;
f. enviar un mensaje de actualizar ubicación a un registro de ubicación local (406) en la HPLMN de la unidad de comunicación de telefonía móvil inalámbrica (401);
g. recibir un mensaje de reconocimiento de actualizar ubicación del registro de ubicación local (406).

7. El nodo de soporte de servicio de acuerdo con la reivindicación 6, en el que además la unidad de procesamiento está también adaptada para

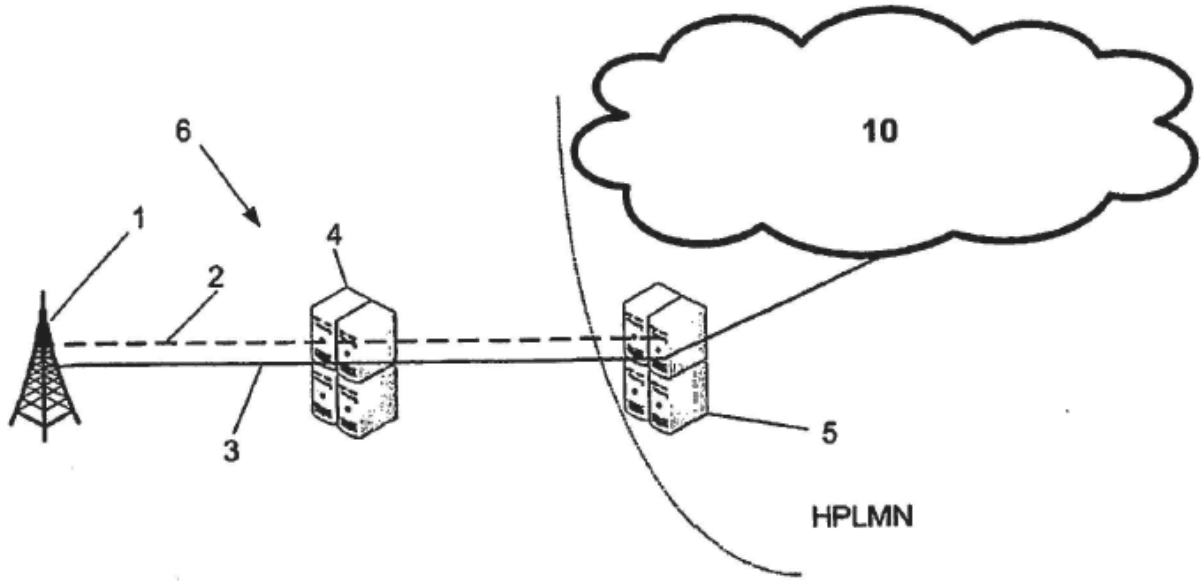
h. recibir un mensaje de cancelar ubicación desde el registro de ubicación local;
i. enviar una solicitud de borrar contexto de PDP reubicado a un primer nodo de soporte de puerta de enlace de proxy (404);
j. recibir una respuesta de borrar contexto de PDP reubicado desde un primer nodo de soporte de puerta de enlace de proxy; y
k. enviar un mensaje de reconocimiento de cancelar ubicación al registro de ubicación local.

8. Un nodo de soporte de puerta de enlace de proxy (409)
para permitir que una unidad de comunicación de telefonía móvil inalámbrica (401) itinere de una primera Red de Telefonía Móvil Terrestre Pública visitada, VPLMN (Visited Public Land Mobile Network, en inglés), VPLMN, (VPLMN1) a una segunda VPLMN, (VPLMN2), comprendiendo la primera VPLMN un primer nodo de soporte de servicio (403) y un primer nodo de soporte de puerta de enlace de proxy (404); comprendiendo la segunda VPLMN el nodo de soporte de servicio (408), constituyendo el segundo nodo de soporte de servicio, y el nodo de soporte de puerta de enlace de proxy (409), que constituye un segundo nodo de soporte de puerta de enlace de proxy, donde se envía carga útil directamente entre una respectiva red de radio de la respectiva VPLMN a un nodo de soporte de puerta de enlace local (405) en una Red de Telefonía Móvil Terrestre Pública Local, HPLMN (Home Public Land Mobile Network, en inglés), HPLMN, a través de respectivos túneles, sin atravesar los nodos de soporte primero y segundo,
el nodo de soporte de puerta de enlace de proxy comprende una unidad de procesamiento (901) adaptada para:

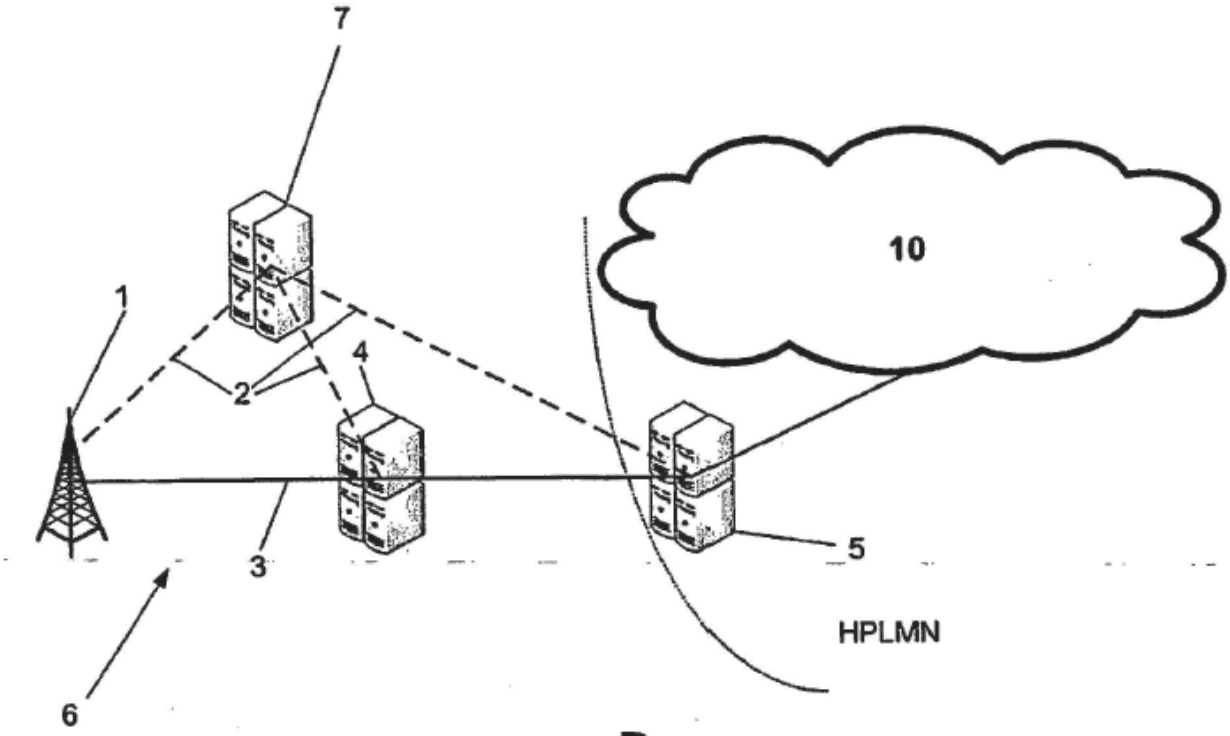
a. recibir una solicitud de reubicar contexto de Protocolo de Datos en Paquetes, es decir, PDP (Packet Data Protocol, en inglés) desde el segundo nodo de soporte de servicio (408);
b. enviar una solicitud de actualizar contexto de PDP al nodo de soporte de puerta de enlace local (405);
c. recibir una respuesta de actualizar contexto de PDP desde el nodo de soporte de puerta de enlace local;
d. enviar una respuesta de reubicar contexto de PDP al segundo nodo de soporte de servicio.

9. El nodo de soporte de puerta de enlace de proxy de acuerdo con la reivindicación 8, en el que además la unidad de procesamiento está adaptada para:

e. recibir una solicitud de borrar contexto de Protocolo de Datos en Paquetes, es decir, PDP (Packet Data Protocol, en inglés) reubicado del primer nodo de soporte de servicio (403); y
f. enviar una respuesta de borrar contexto de PDP reubicado al primer nodo de soporte de servicio.



A



B

Fig. 1

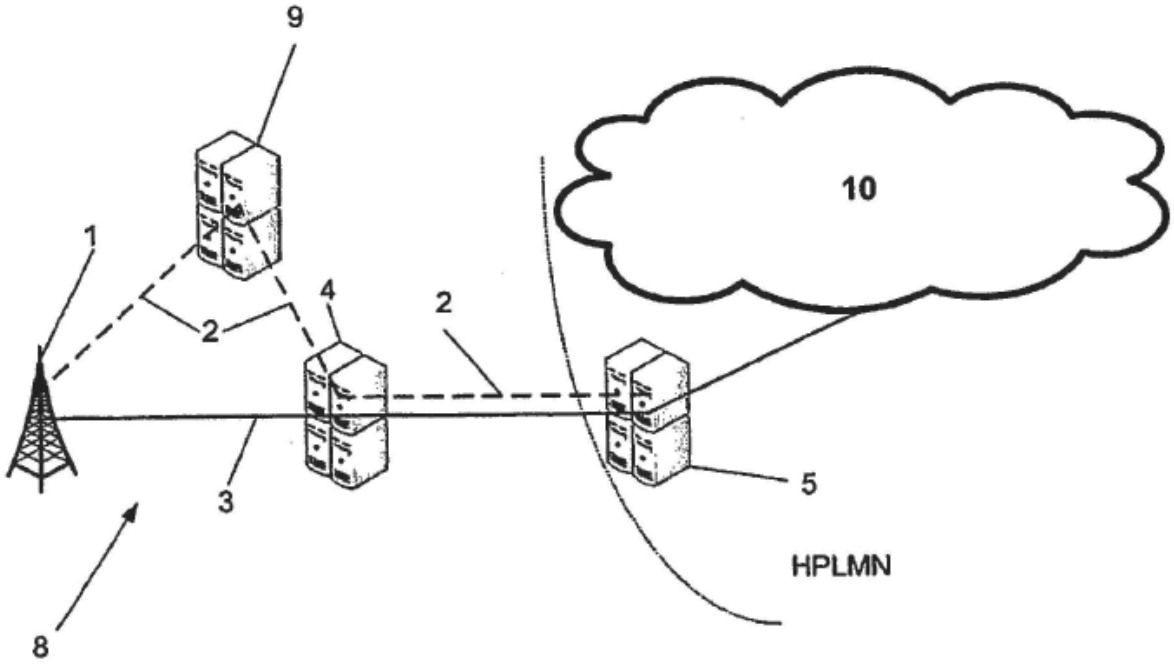


Fig. 2

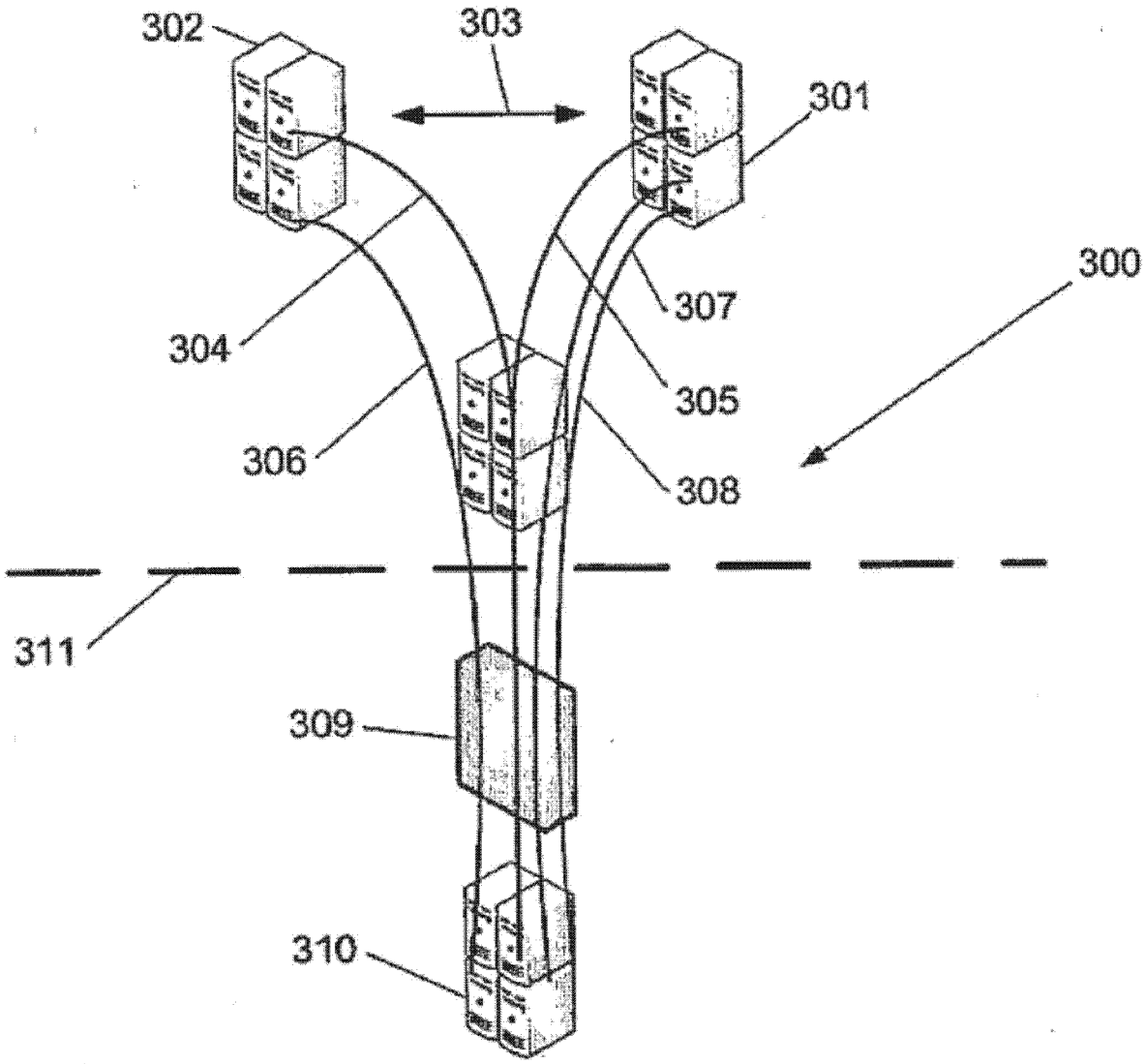


Fig. 3

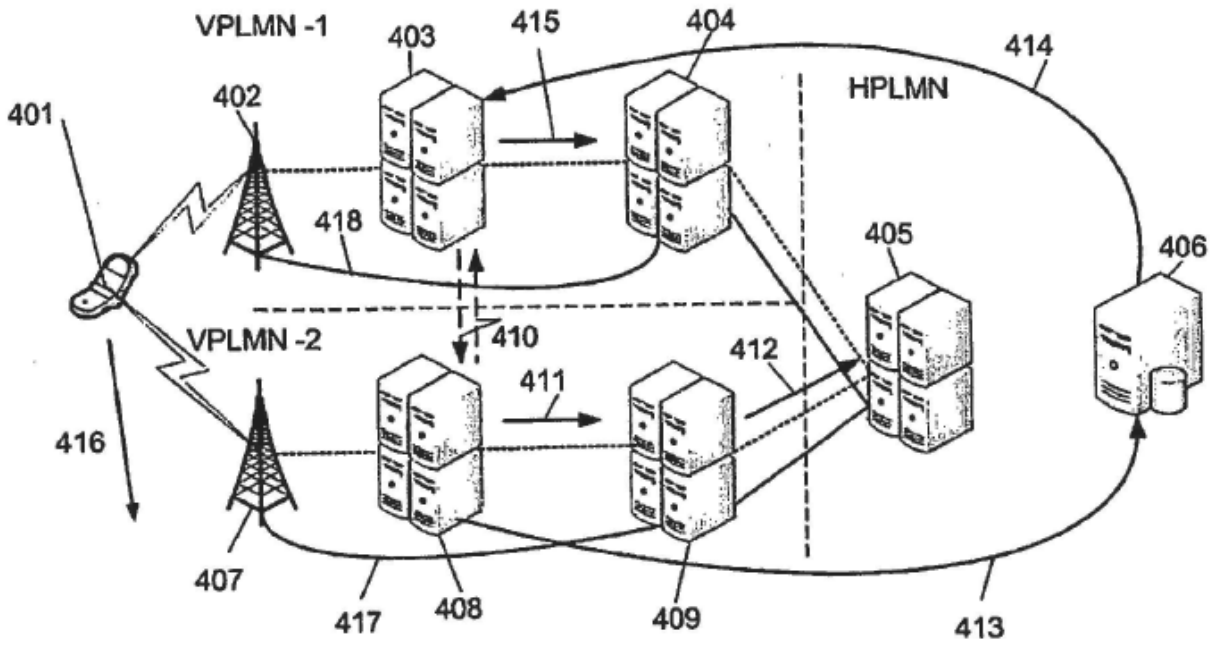

VPLMN -1
403
415
404
414
HPLMN
401
402
418
405
406
VPLMN -2
410
412
411
416
407
417
408
409
413

Fig. 4a

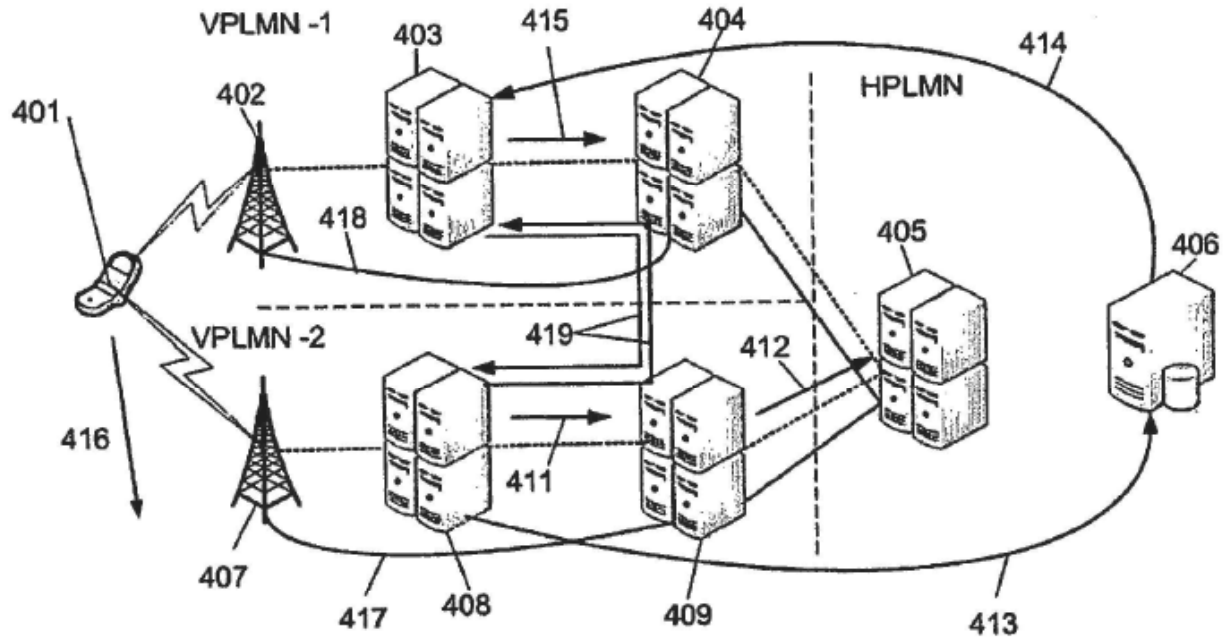

VPLMN -1
403
415
404
414
HPLMN
401
402
418
405
406
VPLMN -2
419
412
416
411
407
417
408
409
413

Fig. 4b

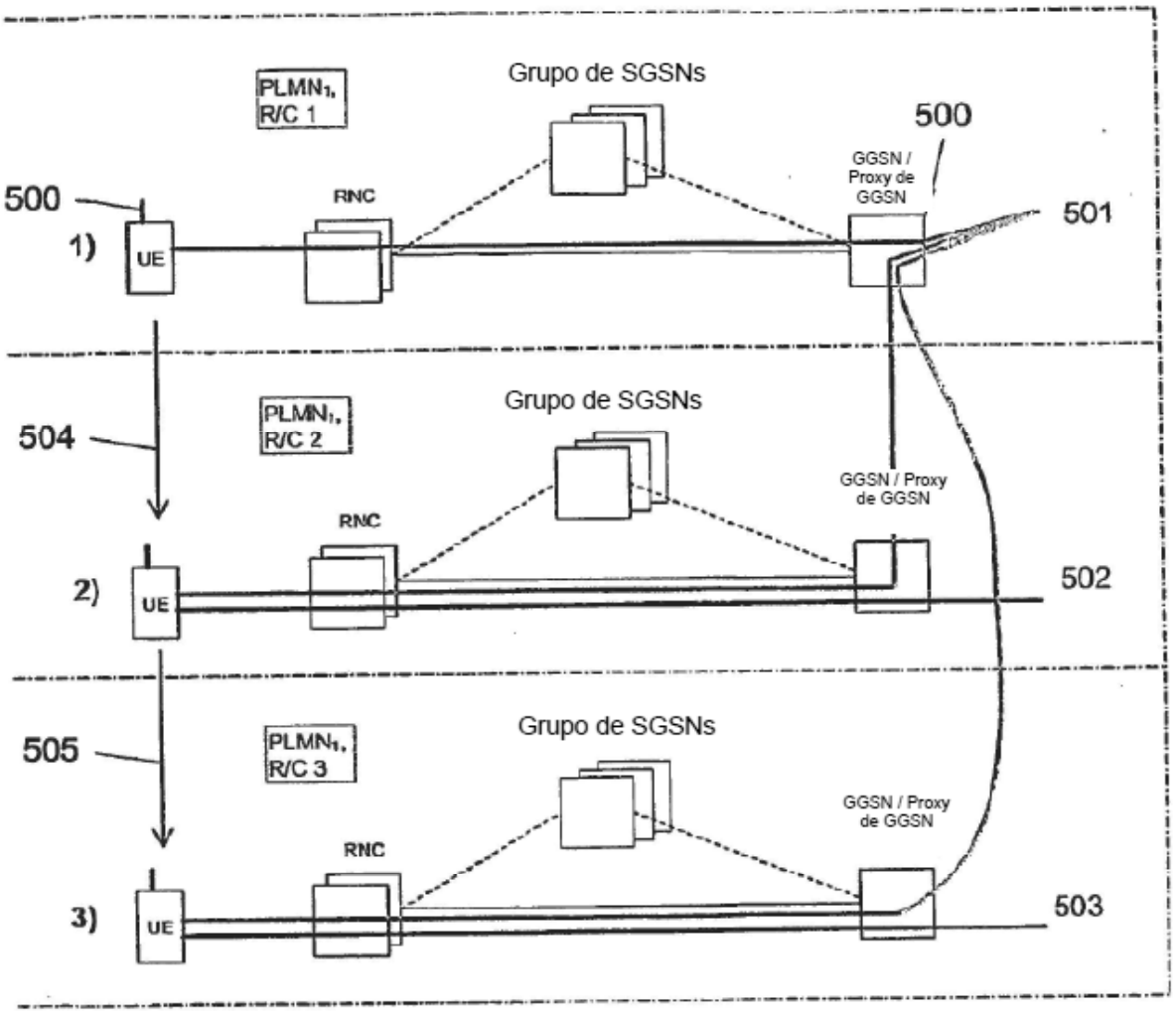

PLMN1, R/C 1
Grupo de SGSNs
500
GGSN / Proxy de GGSN
500
RNC
501
1)
UE
504
PLMN1, R/C 2
Grupo de SGSNs
GGSN / Proxy de GGSN
RNC
2)
UE
502
505
PLMN1, R/C 3
Grupo de SGSNs
GGSN / Proxy de GGSN
RNC
3)
UE
503

Fig. 5

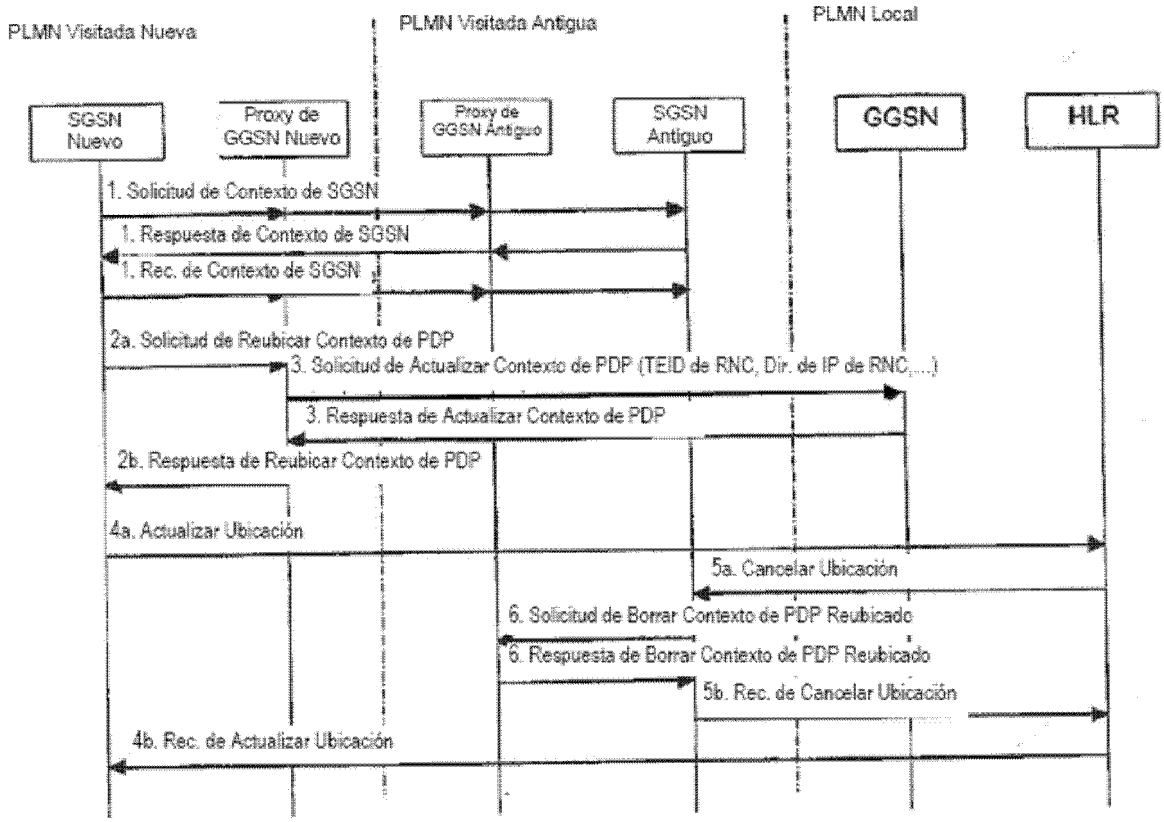

PLMN Visitada Nueva
PLMN Visitada Antigua
PLMN Local
SGSN Nuevo
Proxy de GGSN Nuevo
Proxy de GGSN Antiguo
SGSN Antiguo
GGSN
HLR
1. Solicitud de Contexto de SGSN
1. Respuesta de Contexto de SGSN
1. Rec. de Contexto de SGSN
2a. Solicitud de Reubicar Contexto de PDP
3. Solicitud de Actualizar Contexto de PDP (TEID de RNC, Dir. de IP de RNC,...)
3. Respuesta de Actualizar Contexto de PDP
2b. Respuesta de Reubicar Contexto de PDP
4a. Actualizar Ubicación
5a. Cancelar Ubicación
6. Solicitud de Borrar Contexto de PDP Reubicado
6. Respuesta de Borrar Contexto de PDP Reubicado
5b. Rec. de Cancelar Ubicación
4b. Rec. de Actualizar Ubicación

Fig. 6

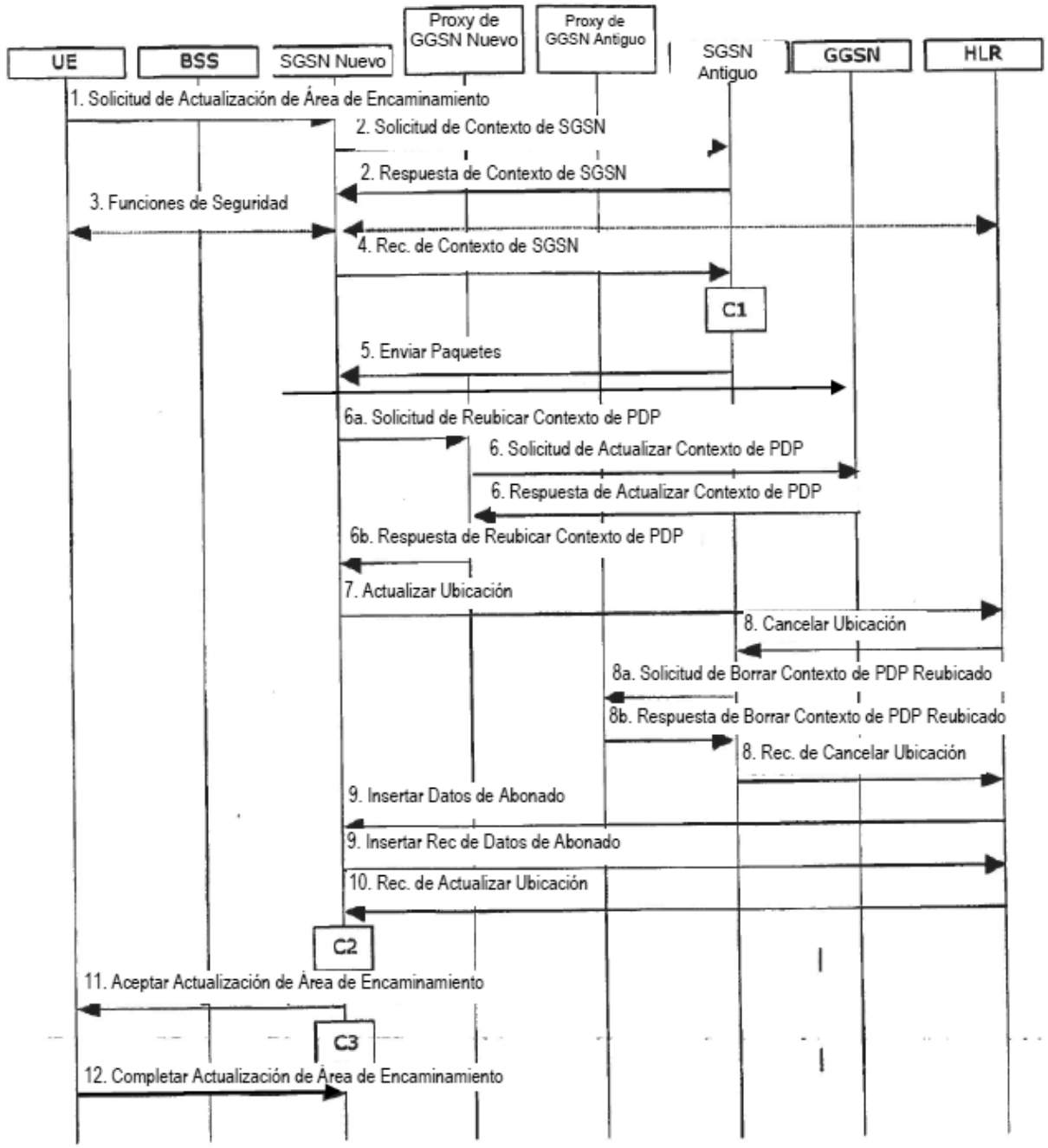

UE
BSS
SGSN Nuevo
Proxy de GGSN Nuevo
Proxy de GGSN Antiguo
SGSN Antiguo
GGSN
HLR
1. Solicitud de Actualización de Área de Encaminamiento
2. Solicitud de Contexto de SGSN
2. Respuesta de Contexto de SGSN
3. Funciones de Seguridad
4. Rec. de Contexto de SGSN
C1
5. Enviar Paquetes
6a. Solicitud de Reubicar Contexto de PDP
6. Solicitud de Actualizar Contexto de PDP
6. Respuesta de Actualizar Contexto de PDP
6b. Respuesta de Reubicar Contexto de PDP
7. Actualizar Ubicación
8. Cancelar Ubicación
8a. Solicitud de Borrar Contexto de PDP Reubicado
8b. Respuesta de Borrar Contexto de PDP Reubicado
8. Rec. de Cancelar Ubicación
9. Insertar Datos de Abonado
9. Insertar Rec de Datos de Abonado
10. Rec. de Actualizar Ubicación
C2
11. Aceptar Actualización de Área de Encaminamiento
C3
12. Completar Actualización de Área de Encaminamiento

Fig. 7

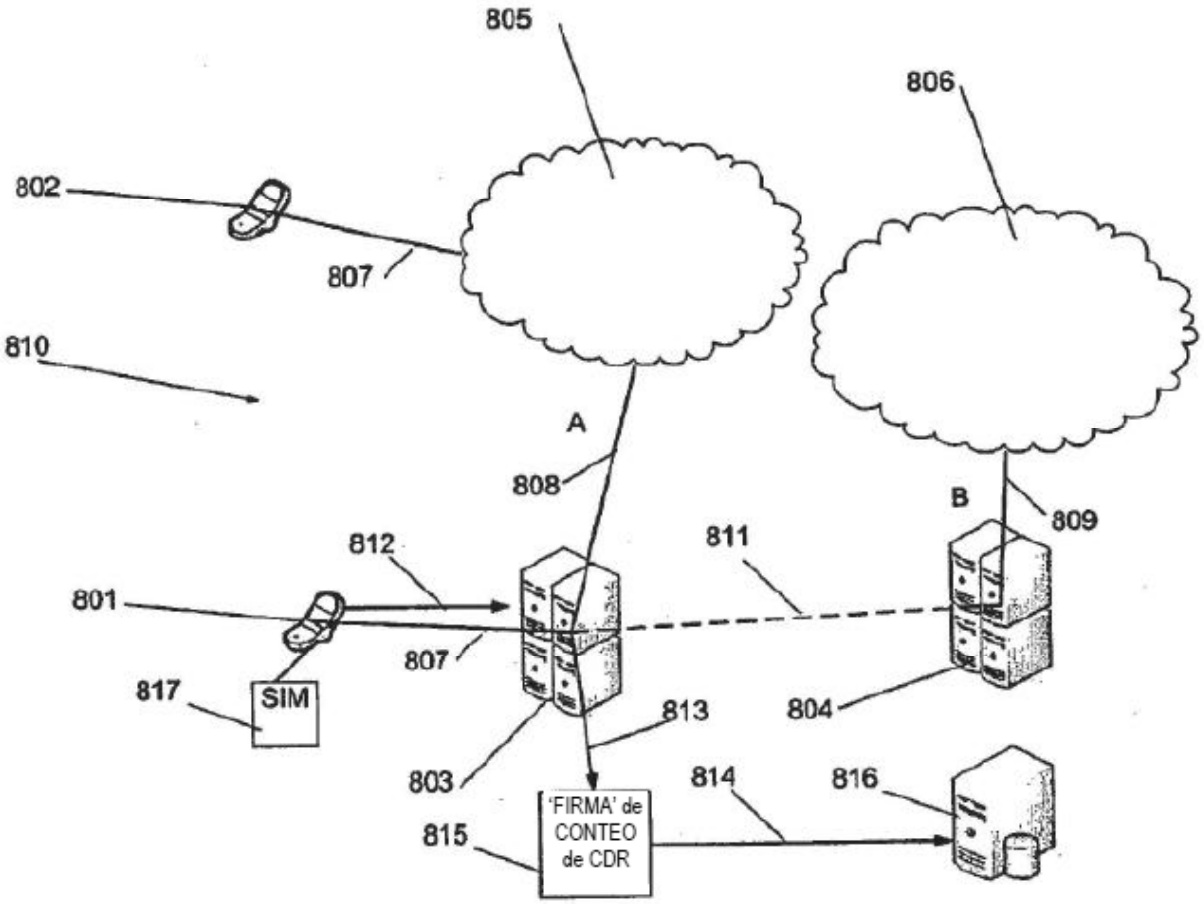

805
806
802
807
810
A
808
B
809
812
811
801
807
817
SIM
804
813
803
814
816
'FIRMA' de CONTEO de CDR
815

Fig. 8

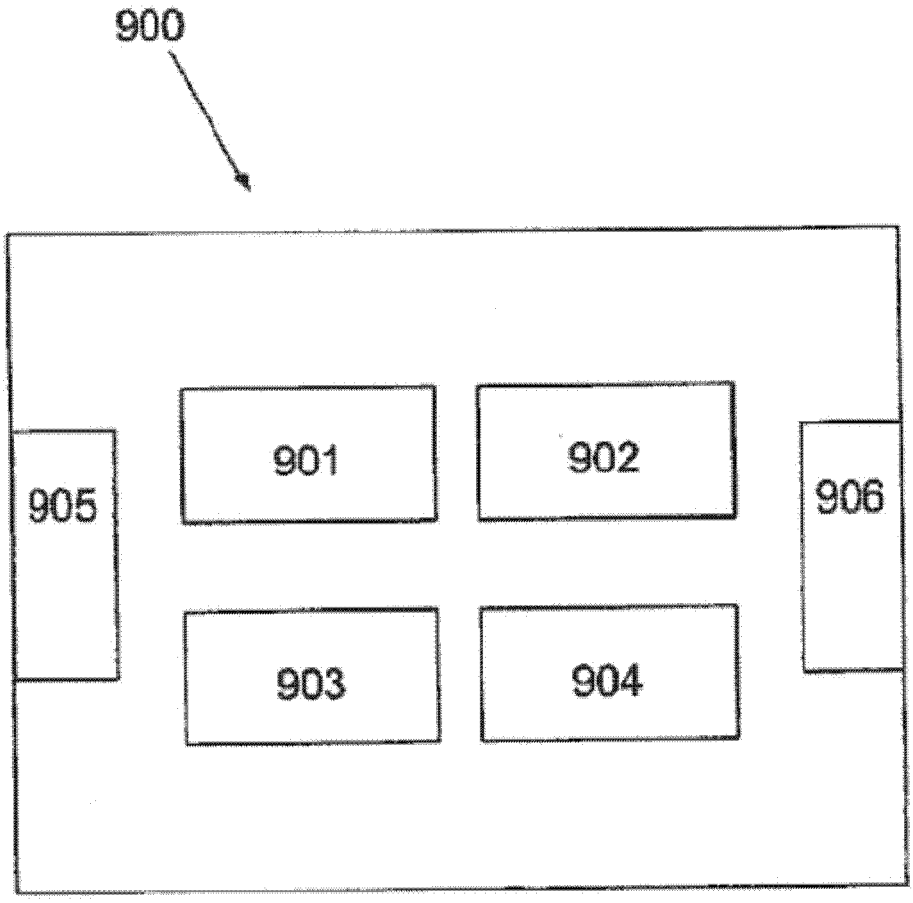


Fig. 9