(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 457 317**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 29/06 (2006.01)
H04W 12/00 (2009.01)
H04W 80/04 (2009.01)
H04W 88/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.10.2008 E 08846173 (6)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2014 EP 2215767**

(54) Título: **Transmisión asegurada de datos en un sistema de comunicaciones**

(30) Prioridad:

01.11.2007 FI 20075780

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.04.2014

(73) Titular/es:

TELIASONERA AB (100.0%)
Stureplan 8
106 63 Stockholm, SE

(72) Inventor/es:

KORHONEN, JOUNI

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Transmisión asegurada de datos en un sistema de comunicaciones

Campo de la invención

La presente invención se refiere a proporcionar un servicio de transmisión asegurada de datos a un terminal de usuario itinerante en un sistema de comunicaciones inalámbricas.

Antecedentes de la invención

Las redes de comunicaciones móviles mejoradas, tales como 3GPP Rel-8, WiMAX Móvil y 3GPP2, darán soporte al protocolo IPv6 móvil delegado como una de las soluciones de movilidad para el tráfico de datos basado en paquetes. El protocolo IPv6 móvil delegado implica a una pasarela de acceso a movilidad (MAG) situada en la red de acceso, para proporcionar acceso a los terminales de usuario, y a un ancla de movilidad local (LMA) situada en la red de origen, que actúa como el encaminador del primer salto y que proporciona acceso a redes externas tales como Internet. Según el protocolo IPv6 móvil delegado, la pasarela de acceso a movilidad (MAG) y el ancla de movilidad local (LMA) comparten una asociación de seguridad (SA). Esto podría, por ejemplo, ser una SA de IPSec. En cada red de acceso, hay normalmente varias pasarelas de acceso a movilidad (MAG). En el IPv6 móvil convencional, las asociaciones de seguridad existen entre un agente de origen y un terminal de usuario. Una diferencia entre el IPv6 móvil delegado y el IPv6 móvil convencional es que, en el IPv6 móvil convencional, el terminal de usuario pertenece a un abonado del operador de origen, y la asociación de seguridad es comprobada, incluso en los casos de itinerancia, durante una verificación normal de la condición de cliente. De manera que la asociación de seguridad (SA) tiene que existir en todo caso. En el IPv6 móvil delegado, la pasarela de acceso a movilidad no pertenece al operador de la red de origen, sino a un socio itinerante. La SA es entre la MAG y la LMA, no entre el terminal de usuario y la LMA. Un terminal itinerante es autenticado y autorizado ante el operador de origen antes de permitirle anexarse a la MAG, ya que la LMA confía en todo terminal que accede a redes externas desde una MAG con la cual tiene una SA.

Uno de los problemas asociados a la disposición precedente es que, especialmente en casos de itinerancia, la gestión de las asociaciones de seguridad es problemática. Por ejemplo, si un operador tiene 100 MAG componentes y 250 socios itinerantes, tiene que haber 25.000 asociaciones de seguridad, simplemente para la itinerancia – en el peor caso, para cada ancla de movilidad local (LMA). Estas SA son además de las SA de abono normal que el operador de origen tiene con cada uno de sus abonados. Técnicamente, este es un problema administrativo, así como un problema de ajustabilidad a escala, especialmente en los casos de itinerancia. Cada pasarela de acceso a movilidad (MAG) incorporada a la red de acceso requiere una nueva asociación de seguridad y la verificación por la conexión de itinerancia. Además, si el operador añade, quita y / o cambia la MAG, los socios itinerantes tienen que acordar una nueva asociación de seguridad (SA) con la MAG añadida, quitada y / o cambiada. Otra desventaja asociada a las soluciones actuales es que requieren un cierto número de configuraciones estáticas. Como cada conexión LMA-MAG implica una asociación de seguridad propia, los cambios en la red de origen son reflejados pronto en los socios de interconexión e itinerancia. Si se cambia algo, la asociación de seguridad ha de ser actualizada. Incluso si la creación de las SA entre MAG y LMA puede ser dinámica, en un entorno de itinerancia esta clase de disposiciones tienden a ser configuradas estáticamente. En el caso de una SA creada dinámicamente (p. ej., usando la negociación de IKEv2), aún queda la complejidad de la distribución de credenciales.

El artículo de Mohanty et al. “Análisis de prestaciones de una arquitectura novedosa para integrar sistemas inalámbricos heterogéneos” (Editores de redes de ordenadores, editores de ciencia Elsevier B. V., Amsterdam, vol. 51, nº 4, 28.12.2006, págs. 1095 a 1105) revela una arquitectura basada en agentes de interoperación de red (NIA) para sistemas inalámbricos heterogéneos. El uso de una unidad de autenticación de un NIA (AU_NIA) elimina la necesidad de cualquier asociación / acuerdo directo de seguridad entre una red ajena y una red de origen. Una vez que el usuario está autenticado, la AU_NIA crea asociaciones / claves de seguridad requeridas entre distintas entidades de red.

El documento oficial IR.34 de la asociación GSM, “Directrices de redes troncales de IP entre proveedores de servicios”, versión 4.1, 31.1.2007, págs. 1 a 45, revela una solución de seguridad y filtrado donde se supone que los proveedores de servicios y los proveedores de IPX garantizan que todos los datagramas de IP del UE (Equipo de Usuario) están encapsulados en túneles para impedir que la red IPX sea accesible por parte de los usuarios finales.

El documento 3GPP TR 33.810, V6.0.0, 1.12.2002, págs. 1 a 27, se refiere a la autenticación de elementos de red que están usando NDS/IP, y situados en un dominio entre operadores. Para un caso de claves secretas manualmente distribuidas, se revela un enfoque de eje-y-rayos, donde cada SEG (pasarela de seguridad) del operador comparte una clave secreta con solamente una pasarela intermedia de seguridad, actuando como un puente para todas las SEG.

El documento US 2004 / 158 706 A1 revela una solución donde se usan túneles criptográficos entre un nodo de origen y un nodo de destino, con paradas intermedias en uno o más nodos repetidores, para enviar y recibir paquetes.-->p. 2A

Breve descripción de la invención

Es por tanto un objeto de la presente invención proporcionar un procedimiento, un sistema y un nodo de red para implementar el procedimiento, a fin de aliviar de tal modo las desventajas precedentes. Los objetos de la invención son logrados por un procedimiento y una disposición que están caracterizados por lo que se asevera en las reivindicaciones independientes. Las realizaciones preferidas de la invención son reveladas en las reivindicaciones dependientes.

La presente invención implica introducir un nodo concentrador en una red de operador de interconexión, en un sistema de comunicaciones que implementa un protocolo IPv6 móvil delegado. La presente invención implica adicionalmente establecer una primera asociación de seguridad individual entre un nodo ancla situado en una red del operador de origen y el nodo concentrador, en donde el nodo concentrador es un nodo delegado; establecer una segunda asociación de seguridad individual entre un nodo de acceso, situado en una red de operador de itinerancia, y el nodo concentrador; y transmitir tráfico de datos entre el nodo ancla y uno o más terminales de usuario, itinerantes en la red del operador de itinerancia, de modo que el tráfico de datos transmitido entre el nodo ancla y el nodo concentrador esté asegurado por el uso de la primera asociación de seguridad individual, y el tráfico de datos transmitido entre el nodo de acceso y el nodo concentrador esté asegurado por el uso de la respectiva segunda asociación de seguridad individual, en donde la red del operador de origen es la red de origen de dichos uno o más terminales de usuario, que están representados por la misma primera asociación de seguridad individual entre el nodo concentrador y el nodo ancla.

Una ventaja del procedimiento y la disposición de la invención es que el número de asociaciones de seguridad necesarias en el sistema puede ser reducido significativamente. En lugar de un enorme número de asociaciones de seguridad, la red del operador de origen solamente necesita acordar una única SA entre el nodo ancla y el nodo concentrador, a fin de gestionar los casos de itinerancia.

Breve descripción de los dibujos

En lo que sigue, la invención será descrita en mayor detalle por medio de realizaciones preferidas, con referencia a los dibujos adjuntos, en los cuales

la Figura 1 ilustra la arquitectura general de un sistema de comunicación según una realización de la presente solución;

la Figura 2 ilustra la señalización según una primera realización de la presente solución;

la Figura 3 ilustra la señalización según una segunda realización de la presente solución;

la Figura 4 es un diagrama de flujo que ilustra la funcionalidad de un nodo ancla según una realización de la presente solución;

la Figura 5 es un diagrama de flujo que ilustra la funcionalidad de un nodo de acceso según una realización de la presente solución;

la Figura 6 es un diagrama de flujo que ilustra la funcionalidad de un nodo concentrador según una realización de la presente solución,

y la Figura 7 es un diagrama de flujo que ilustra la funcionalidad de un nodo concentrador según una realización de la presente solución.

Descripción detallada de la invención

En lo que sigue, las realizaciones de la invención serán descritas con referencia a un sistema avanzado de comunicaciones móviles celulares, tal como 3GPP Rel-8, 3GPP2 o WiMAX Móvil. Sin embargo, la invención no está concebida para restringirse a estas realizaciones. La presente invención es aplicable a cualquier nodo de red, el componente, o los componentes, correspondiente(s) y / o cualquier sistema de comunicación, o cualquier combinación de distintos sistemas de comunicación capaces de proporcionar la transmisión de datos conmutados por paquetes, tales como 4G, Beyond-3G o WLAN. El sistema de comunicación puede ser un sistema de comunicación fija, un sistema de comunicación inalámbrica o un sistema de comunicación que utilice tanto redes fijas como redes inalámbricas. Los protocolos usados y las especificaciones de sistemas de comunicación y de nodos de red, especialmente en la comunicación móvil e inalámbrica, evolucionan rápidamente. Tal evolución puede requerir cambios extra en una realización. Por lo tanto, todas las palabras y expresiones deberían ser interpretadas en sentido amplio, y están concebidas para ilustrar, no para restringir, la realización. El aspecto inventivo relevante es la funcionalidad concernida, no el elemento de red o el equipo donde es ejecutada.

Una asociación de seguridad (SA) se refiere a una conexión entre dos o más entidades de redes de comunicaciones, que describe cómo las entidades utilizarán los servicios de seguridad a fin de comunicarse con seguridad. La asociación de seguridad define cuáles transformaciones y algoritmos son usados en una cabecera de autenticación, o carga útil de seguridad encapsuladora, para proporcionar servicios de seguridad para el tráfico de datos que lleva.

Una red de intercambio de itinerancia del GPRS (GRX) se refiere a una red centralizada de encaminamiento de IP que interconecta redes del servicio general de radio en paquetes (GPRS), y que permite una cobertura global de itinerancia para redes inalámbricas, directamente, o mediante otras redes de GRX. El GRX está definido en el documento GSMA PRD IR.34.

La interoperabilidad mundial para el acceso por microondas (WiMAX) se refiere a una tecnología para redes inalámbricas que funciona según una norma IEEE 802.16. WiMAX es una tecnología de red de área metropolitana inalámbrica que proporciona una conexión de acceso de banda ancha del último tramo, desde puntos de acceso de red de área local inalámbrica (WLAN) a Internet. WiMAX es complementaria para las WLAN y la fidelidad inalámbrica (Wi-Fi), proporcionando un ancho de banda aumentado y una más amplia cobertura inalámbrica.

La presente solución se basa en la idea de introducir un nodo concentrador, tal como un concentrador del IPv6 móvil delegado, en una red que implemente el protocolo IPv6 móvil delegado. La presente solución permite una solución de concentrador / agente usando el protocolo IPv6 móvil delegado para redes de interconexión, donde el tráfico de datos de itinerancia es transferido por encima del protocolo IPv6 móvil delegado. La presente solución introduce un concentrador del IPv6 móvil delegado en la red de interconexión, que está gestionado por el operador preferido de la red de interconexión. Aquí, la red de interconexión se refiere, por ejemplo, a una red de intercambio de itinerancia del GPRS (GRX), o sus evoluciones, tales como IPX (Intercambio de paquetes de Internet, según lo definido en el documento GSMA PRD IR.34). La presente solución se basa en la idea de que un operador de red de origen tiene una única conexión con el concentrador, y el concentrador está conectado con la pasarela de acceso a movilidad (MAG) del socio de itinerancia. De ese modo, las conexiones de itinerancia están detrás de un único concentrador alojado, por ejemplo, por el proveedor de red de GRX al usar el protocolo IPv6 móvil delegado. La ubicación del concentrador no está ligada al GRX, aunque es un lugar factible para desplegar un nodo concentrador de ese tipo. El concentrador del IPv6 móvil delegado, según la presente solución, aparece lógicamente como una pasarela de acceso a movilidad (MAG) para un ancla de movilidad local (LMA) situada en la red de origen y, entre la LMA y el concentrador, solamente se necesita una única asociación de seguridad (SA). El resto del tráfico se dispone de modo que se acuerde una asociación de seguridad adicional entre el concentrador y la pasarela de acceso a movilidad (MAG). De manera similar, el concentrador del IPv6 móvil delegado aparece como una LMA para una MAG. Una única SA también se necesita en este caso, entre el concentrador y la MAG. Los múltiples concentradores del IPv6 móvil delegado pueden estar interconectados (encadenados) entre sí, creando así una red de concentradores (mallas).

En lo que sigue, las realizaciones de la presente solución serán descritas con referencia a los dibujos adjuntos.

La Figura 1 ilustra un sistema S de comunicaciones según una realización. Con referencia a la Figura 1, el sistema S comprende al menos un terminal UE1-2, UE1-3, UE1-4, UE1-5 de usuario que puede ser, p. ej., un terminal móvil o un terminal inalámbrico, tal como un teléfono móvil (estación móvil), un asistente digital personal (PDA), una consola de juegos, un ordenador portátil o similares, capaces de funcionar en una red de comunicaciones conmutada por paquetes. El sistema S comprende además al menos una red N1, N2, N3, N4, N5 de acceso, tal como una red de área local inalámbrica (WLAN), o una red de acceso por radio (RAN) de una red celular. Aquí se supone que las redes N1, N2, N3, N4, N5 de acceso son operadas por distintos operadores de red, siendo la red N1 de acceso la red del operador de origen del terminal UE1-2, UE1-3, UE1-4, UE1-5 de usuario, e incluyendo un ancla de movilidad local LMA1 (también denominada nodo ancla). En la situación mostrada en la Figura 1, el terminal UE1-2 de usuario es itinerante en la red N2 de acceso, el terminal UE1-3 de usuario es itinerante en la red N3 de acceso, el terminal UE1-4 de usuario es itinerante en la red N4 de acceso y el terminal UE1-5 de usuario es itinerante en la red N5 de acceso. La red N2, N3, N4, N5 de acceso (también denominada una red de operador de itinerancia) incluye al menos una correspondiente pasarela de acceso a movilidad (también denominada un nodo de acceso) MAG2, MAG3, MAG4, MAG5 para proporcionar acceso al terminal UE1-2, UE1-3, UE1-4, UE1-5 de usuario mediante la correspondiente red N2, N3, N4, N5 de acceso. Aquí se supone que los nodos MAG2, MAG3, MAG5 de acceso son capaces de conectarse con la LMA1 mediante una primera red GRXa de intercambio de itinerancia del GPRS. Se supone además que los nodos MAG4, MAG5 de acceso son capaces de conectarse con la LMA1 mediante la primera red GRXb de intercambio de itinerancia del GPRS y una segunda red GRXb de intercambio de itinerancia del GPRS, ambas combinadas. La primera red GRXa de intercambio de itinerancia del GPRS incluye un primer nodo concentrador Ha (tal como un concentrador del IPv6 móvil delegado) según la presente solución, y la segunda red GRXb de intercambio de itinerancia del GPRS incluye un segundo nodo concentrador Hb (tal como un concentrador del IPv6 móvil delegado) según la presente invención. En la Figura 1, una primera asociación SA1 de seguridad, según la presente solución, ha sido establecida entre la LMA1 y el Ha, y una segunda asociación SA2, SA3, SA4, SA5 de seguridad, según la presente solución, ha sido establecida, respectivamente, entre 1) el Ha y la MAG2, 2) el Ha y la MAG3, 3) el Hb y la MAG4 y 4) el Hb y la MAG5. El terminal UE1-2, UE1-3, UE1-4, UE1-5 de usuario puede obtener acceso a los servicios E externos de red, mediante su red N1 de origen, usando la primera asociación SA1 de seguridad y la segunda asociación SA2, SA3, SA4, SA5 de seguridad adecuada. La Figura 1 muestra una versión simplificada de la estructura de red, que ilustra solamente los componentes que son esenciales para ilustrar la presente solución, incluso aunque los expertos en la técnica saben naturalmente que un sistema general de comunicaciones también comprende otras funciones y estructuras, que no tienen que ser descritas en mayor detalle en la presente memoria. El nodo LMA1 de

red puede incluir a cualquier elemento de red operado por un operador de red de origen, para proporcionar movilidad para el terminal de usuario, tal como un nodo de soporte del GPRS de pasarela (GGSN), una pasarela de red de datos en paquetes (PDN-GW) o cualquier agente de origen capacitado para el IPv6 móvil delegado. Los nodos MAG2, MAG3, MAG4, MAG5 de red pueden incluir cualquier elemento de red operado por un operador de red de itinerancia, para rastrear el terminal de usuario en la red de itinerancia. La MAG también funciona como un servidor de acceso a red para el terminal, y el terminal ha de ser autenticado / autorizado mediante la MAG ante la red del operador de origen. Puede haber varias alternativas para llevar a cabo la autenticación y / o autorización, según la tecnología de acceso. Por ejemplo, con relación a WiMAX, puede llevarse a cabo una autenticación basada en EAP, donde la MAG (es decir, la ASN-GW en WiMAX) funciona como el autenticador, remitiendo la autenticación a un servidor de AAA (autenticación, autorización y registro) del operador de origen, usando un protocolo de AAA seleccionado. Los nodos Ha, Hb de red pueden incluir cualquier elemento de red operado por un operador de red de interconexión, para proporcionar una conexión entre redes de acceso y redes de interconexión, tal como un concentrador. El concentrador puede incluir, por tanto, una funcionalidad de encaminador, una funcionalidad de GW de IPSec y probablemente también una funcionalidad de cliente de AAA. Aunque cada nodo LMA1, MAG2, MAG3, MAG4, MAG5, Ha, Hb de red ha sido ilustrado como una entidad, distintos módulos y memorias pueden ser implementados en una o más entidades físicas o lógicas.

Las Figuras 2 y 3 ilustran la señalización según realizaciones de la presente solución.

Según una primera realización de la presente solución, con referencia a la Figura 2, una primera asociación SA1 de seguridad está establecida 2-1 entre el ancla de movilidad local LMA1 (nodo ancla) situada en la red N1 del operador de origen del terminal UE1-2 de usuario, y el nodo concentrador Ha (concentrador del IPv6 móvil delegado) situado en la red GRXa del operador de interconexión. Una segunda asociación SA2 de seguridad está establecida 2-2 entre el nodo concentrador Ha situado en la red GRXa del operador de interconexión y la pasarela de acceso a movilidad MAG2 (nodo de acceso) situada en la red N2 del operador de itinerancia. Durante el establecimiento, los nodos LMA1 y Ha de red, y Ha y MAG2, pueden intercambiar información sobre qué clase de protocolo de seguridad ha de ser usado para la red de origen y la red de itinerancia en cuestión. Cualquier procedimiento de señalización existente puede ser utilizado cuando la asociación SA1, SA2 de seguridad está establecida. El terminal UE1-2 de usuario (situado en la N2) transmite 2-3 tráfico de datos dirigido a la red externa E. Los datos son recibidos en el nodo MAG2 de acceso, que remite 2-4 los datos al nodo concentrador Ha utilizando la segunda asociación SA2 de seguridad, según la primera realización de la presente solución. Los datos son recibidos en el nodo concentrador Ha, que remite 2-5 los datos al nodo ancla LMA1, utilizando la primera asociación SA1 de seguridad, según una realización de la presente solución. Según el tráfico de datos es recibido en el nodo ancla LMA1, el nodo ancla LMA1 remite 2-6 los datos a la red externa E (p. ej., Internet). En el mensaje 2-7, el tráfico de datos dirigido al terminal UE1-2 de usuario itinerante es transmitido desde la red externa E al nodo ancla LMA1. Los datos son recibidos en el LMA1, que los remite 2-8 al nodo concentrador Ha utilizando la primera asociación SA1 de seguridad, según la primera realización de la presente solución. Los datos son recibidos en el nodo concentrador Ha, que los remite 2-9 al nodo MAG2 de acceso utilizando la segunda asociación SA2 de seguridad, según la primera realización de la presente solución. Según el tráfico de datos es recibido en el nodo MAG2 de acceso, el nodo MAG2 de acceso remite 2-10 los datos al terminal UE1-2 de usuario. Debería observarse que la transmisión de datos entre la red externa E y el terminal UE1-3 de usuario es llevada a cabo de la misma manera, pero en este caso el nodo de acceso a usar es MAG3, y la segunda asociación de seguridad a usar es SA3 (establecida entre Ha y MAG3).

Según una segunda realización de la presente solución, con referencia a la Figura 3, una primera asociación SA1 de seguridad es establecida 3-1 entre el ancla de movilidad local LMA1 (nodo ancla) situada en la red N1 del operador de origen del terminal UE1-4 de usuario, y el primer nodo concentrador Ha (concentrador del IPv6 móvil delegado) situado en la primera red GRXa del operador de interconexión. Una segunda asociación SA4 de seguridad es establecida 3-2 entre el segundo nodo concentrador Hb (concentrador del IPv6 móvil delegado) situado en la segunda red GRXb del operador de interconexión y la pasarela de acceso a movilidad MAG4 (nodo de acceso) situada en la red N4 del operador de itinerancia. Durante el establecimiento, los nodos LMA1 y Ha de red, y Ha y MAG2, pueden intercambiar información sobre qué clase de protocolo de seguridad ha de usarse para la red de origen y la red de itinerancia en cuestión. Cualquier procedimiento de señalización existente puede utilizarse cuando la asociación SA1, SA2 de seguridad está establecida. El terminal UE1-4 de usuario (situado en la N4) transmite 3-3 tráfico de datos dirigido a la red externa (E). Los datos son recibidos en el nodo MAG4 de acceso, que remite 3-4 los datos al segundo nodo concentrador Hb, utilizando la segunda asociación SA4 de seguridad, según la segunda realización de la presente solución. Los datos son recibidos en el segundo nodo concentrador Hb, que remite 3-5 los datos al primer nodo concentrador Ha. Según los datos son recibidos en el primer nodo concentrador Ha, el primera nodo concentrador Ha remite 3-6 los datos al nodo ancla LMA1, utilizando la primera asociación SA1 de seguridad, según una realización de la presente solución. Según el tráfico de datos es recibido en el nodo ancla LMA1, el nodo ancla LMA1 remite 3-7 los datos a la red externa E (p. ej., Internet). En el mensaje 3-8, el tráfico de datos dirigido al terminal UE1-4 de usuario itinerante es transmitido desde la red externa E al nodo ancla LMA1. Los datos son recibidos en la LMA1, que los remite 3-9 al primer nodo concentrador Ha, utilizando la primera asociación SA1 de seguridad, según la segunda realización de la presente solución. Los datos son recibidos en el primer nodo concentrador Ha, que los remite 3-10 al

segundo nodo concentrador Hb. Según los datos son recibidos en el segundo nodo concentrador Hb, el segundo nodo concentrador Hb remite 3-11 los datos al nodo de acceso MAG4, utilizando la segunda asociación SA4 de seguridad, según la segunda realización de la presente solución. Según el tráfico de datos es recibido en el nodo de acceso MAG4, el nodo de acceso MAG4 remite 3-12 los datos al terminal UE1-2 de usuario. Debería observarse que la transmisión de datos entre la red externa E y el terminal UE1-5 de usuario es llevada a cabo de la misma manera, pero en este caso el nodo de acceso a usar es MAG5, y la segunda asociación de seguridad a usar es SA5 (establecida entre Hb y MAG5).

Las Figuras 4, 5, 6 y 7 ilustran la funcionalidad de los nodos de red según las realizaciones de la presente solución.

La Figura 4 ilustra la funcionalidad del nodo ancla LMA1 (tal como un ancla de movilidad local) según una realización de la presente solución. Con referencia a la Figura 4, la primera asociación SA1 de seguridad es establecida, en la etapa 4-1, con el primer nodo concentrador Ha (tal como un concentrador del IPv6 móvil delegado) situado en la red GRXa del operador de interconexión. En la etapa 4-2, el tráfico de datos dirigido a la red externa E es recibido desde el primer nodo concentrador Ha, utilizando la primera asociación SA1 de seguridad. En la etapa 4-3, el tráfico de datos recibidos es remitido a la red externa E. En la etapa 4-4, el tráfico de datos dirigido al terminal UE1-2, UE1-3, UE1-4, UE1-5 de usuario itinerante es recibido desde la red externa E. En la etapa 4-5, el tráfico de datos recibido es remitido al primer nodo concentrador Ha, utilizando la primera asociación SA1 de seguridad.

La Figura 5 ilustra la funcionalidad del nodo MAG2 de acceso (tal como una pasarela de acceso a movilidad) según una realización de la presente solución. Con referencia a la Figura 5, la segunda asociación SA2 de seguridad es establecida, en la etapa 5-1, con el nodo concentrador Ha (tal como un concentrador del IPv6 móvil delegado) situado en la red GRXa del operador de interconexión. En la etapa 5-2, el tráfico de datos dirigido a la red externa E es recibido desde el terminal UE1-2 de usuario itinerante utilizando la segunda asociación SA2 de seguridad. En la etapa 5-3, el tráfico de datos recibido es remitido al nodo concentrador Ha. En la etapa 5-4, el tráfico de datos dirigido al terminal UE1-2 de usuario itinerante es recibido desde el nodo concentrador Ha. En la etapa 5-5, el tráfico de datos recibido es remitido al terminal UE1-2 de usuario utilizando la primera asociación SA1 de seguridad. Debería observarse que la funcionalidad de MAG3 está implementada en consecuencia, pero en ese caso el terminal es UE1-3, y la segunda asociación de seguridad es SA3 (establecida entre Ha y MAG3). También debería observarse que la funcionalidad de MAG4, MAG5 está implementada en consecuencia, pero en ese caso el terminal de usuario es UE1-4, UE1-5, y la segunda asociación de seguridad es, respectivamente, SA4, SA5 (establecida entre Hb y MAG4, MAG5).

La Figura 6 ilustra la funcionalidad del nodo concentrador Ha (tal como un concentrador del IPv6 móvil delegado) según una primera realización de la presente solución. Con referencia a la Figura 6, la primera asociación SA1 de seguridad es establecida, en la etapa 6-1, con el nodo ancla LMA1 (tal como un ancla de movilidad local) situado en la red N1 del operador de origen del terminal UE1-2 de usuario. En la etapa 6-2, la segunda asociación SA2 de seguridad es establecida con el nodo MAG2 de acceso (tal como una pasarela de acceso a movilidad) situado en la red N2 del operador de itinerancia. En la etapa 6-3, el tráfico de datos dirigido a la red externa E es recibido desde el nodo MAG2 de acceso, utilizando la segunda asociación SA2 de seguridad. En la etapa 6-4, el tráfico de datos recibido es remitido al nodo ancla LMA1, utilizando la primera asociación SA1 de seguridad. En la etapa 6-5, el tráfico de datos dirigido al terminal UE1-2 de usuario itinerante es recibido desde el nodo ancla LMA1, utilizando la primera asociación SA1 de seguridad. En la etapa 6-6, el tráfico de datos recibido es remitido al nodo MAG2 de acceso, utilizando la segunda asociación SA2 de seguridad. Debería observarse que la transmisión de datos entre la red externa E y el terminal UE1-3 de usuario es llevada a cabo en consecuencia, pero en ese caso el nodo de acceso a usar es MAG3, y la segunda asociación de seguridad a usar es SA3 (establecida entre Ha y MAG3). También debería observarse que en la segunda realización de la presente solución, la transmisión de datos entre la red externa E y el terminal UE1-4, UE1-5 de usuario itinerante es llevada a cabo en consecuencia, pero en ese caso el primer nodo concentrador Ha recibe el tráfico de datos dirigido a la red externa E, desde el segundo nodo concentrador Hb (en lugar del nodo de acceso), y el primer nodo concentrador Ha remite el tráfico de datos dirigido al terminal UE1-4, UE1-5 de usuario itinerante al segundo nodo concentrador Hb (en lugar del nodo de acceso).

La Figura 7 ilustra la funcionalidad del segundo nodo concentrador Hb (tal como un segundo concentrador del IPv6 móvil delegado) según una segunda realización de la presente solución. Con referencia a la Figura 7, la segunda asociación SA4 de seguridad es establecida, en la etapa 7-1, con el nodo MAG4 de acceso (tal como una pasarela de acceso a movilidad) situado en la red N4 del operador de itinerancia. En la etapa 7-2, el tráfico de datos dirigido a la red externa E es recibido desde el nodo MAG4 de acceso, utilizando la segunda asociación SA4 de seguridad. En la etapa 7-3, el tráfico de datos recibido es remitido al primer nodo concentrador Ha (tal como un concentrador del IPv6 móvil delegado). En la etapa 7-4, el tráfico de datos dirigido al terminal UE1-4 de usuario itinerante es recibido desde el primer nodo concentrador Ha. En la etapa 7-5, el tráfico de datos recibido es remitido al nodo MAG4 de acceso, utilizando la segunda asociación SA4 de seguridad. Debería observarse que la transmisión de datos entre la red externa E y el terminal UE1-5 de usuario se lleva a cabo en consecuencia, pero en ese caso el nodo de acceso a usar es MAG5, y la segunda asociación de seguridad a usar es SA5 (establecida entre Hb y MAG5).

Debería observarse que la transmisión del tráfico de datos puede ser inicializada por la red externa E (en lugar del

terminal UE1-2, UE1-3, UE1-4, UE1-5 de usuario itinerante), en cuyo caso, por ejemplo, la transmisión de los mensajes 2-7, 2-8, 2-9 y 2-10 es llevada a cabo antes de la transmisión de los mensajes 2-3, 2-4, 2-5 y 2-6.

Debería observarse que la conexión entre Ha y Hb, mediante la cual son remitidos los datos en la segunda realización, puede ser implementada con cualquier técnica adecuada de transmisión de datos. También debería observarse que, además de GRXa y GRXb, si es necesario, pueden ser implicadas una o más redes adicionales de interconexión en la remisión del tráfico de datos entre Ha y Hb. Las redes de interconexión en cuestión son luego responsables de la implementación de la conexión de datos entre distintas redes de interconexión.

Un ejemplo del tráfico de datos desde el terminal de usuario a la red externa es que el terminal de usuario transmite una solicitud de servicio, solicitando un servicio o aplicación de Internet. Un ejemplo del tráfico de datos desde la red externa al terminal de usuario es que un servicio o aplicación de Internet, solicitado por el terminal de usuario, es transmitido al terminal de usuario. La presente solución puede ser aplicada al tráfico de datos del enlace ascendente y / o del enlace descendente. El tráfico de datos puede incluir, por ejemplo, ficheros de música, ficheros de voz, ficheros de datos, voz, etc.

Una ventaja de la invención es que el operador de la red de origen solamente necesita acordar una única asociación SA1 de seguridad en la red de origen y una única asociación SA2 de seguridad en cada red de itinerancia, a fin de disponer conexiones de datos aseguradas para sus abonados itinerantes, usando el protocolo IPv6 móvil delegado.

Aunque la red de origen tiene varios socios de itinerancia, la LMA1 solamente necesita estar conectada con un Ha lógicamente único (en consecuencia, desde el punto de vista de la MAG, la MAG se comunica lógicamente con un único concentrador, aunque el tráfico es transmitido a varias LMA). La SA1 existe entre la LMA1 y el Ha (no entre la LMA1 y cada uno de los nodos MAG2, MAG3, MAG4, MAG5 de acceso, como en las soluciones convencionales). Ha y / o Hb se ocupan de las conexiones de itinerancia y de las asociaciones SA2, SA3, SA4, SA5 de seguridad con los respectivos nodos MAG2, MAG3, MAG4, MAG5 de acceso.

Por medio de la presente solución, a pesar de un enorme número de terminales de usuario referidos al servicio y al protocolo IPv6 móvil delegado, todos los terminales (cuya red de origen es N1) pueden ser representados por la misma SA1 entre Ha y LMA1. En la presente solución, una asociación de seguridad es dividida en dos partes SA1 y SA2 entre el Ha y la LMA1, y el Ha y la MAG2. El protocolo IPv6 móvil delegado permite esto, ya que la asociación de seguridad entre la pasarela de acceso móvil y el nodo ancla local es una asociación de seguridad de IPSec, y la conexión entre ellos es una VPN de IPSec.

En la práctica, el concentrador Ha, Hb no necesita “entender” el protocolo IPv6 móvil delegado. El concentrador desencapsula y encapsula el tráfico de datos entre distintos túneles de IPSec. El tráfico móvil en túneles de IP es transmitido dentro de IPSec, mientras que en el caso del IPv6 el tráfico móvil en túneles de IP puede ser transmitido normalmente, y en el caso del IPv4 puede ser necesario usar un túnel adicional de GRE (encapsulación genérica de encaminamiento) dentro de IPSec, si las direcciones del IPv4 llegan desde el espacio privado. Los datos del plano del usuario son transmitidos dentro del túnel del IP móvil. Los puntos extremos del túnel de IP móvil son la MAG y la LMA y, en base a ese conocimiento, los concentradores terminados por IPSec son capaces de encaminar el tráfico en túneles del IPv6 móvil delegado, en el sentido de IP.

Las ventajas de la presente solución incluyen una alta ajustabilidad a escala desde el punto de vista del operador de la red de origen, y el hecho de que los cambios en el protocolo IPv6 delegado no son necesarios. La solución permite la fácil gestión y configuración de conexiones de itinerancia al usar la tecnología basada en el IPv6 móvil delegado para la itinerancia. Desde el punto de vista del operador de red de interconexión, la presente solución habilita un nuevo modelo de funcionamiento y servicio, en forma del concentrador del IPv6 móvil delegado, según lo descrito anteriormente. De tal modo, la red de interconexión puede aumentar su rentabilidad añadiendo nueva inteligencia y nuevos servicios facturables en su red. La presente solución cambia el modelo convencional de itinerancia. En la presente solución, los acuerdos bilaterales entre los operadores de los usuarios finales ya no son necesarios, pero los pertenecientes a la misma comunidad de itinerancia / interconexión son accesibles entre sí sin acciones especiales. La presente solución permite el despliegue sencillo de disposiciones de itinerancia multilateral desde el punto de vista del operador.

Las asociaciones de seguridad pueden ser establecidas como asociaciones de seguridad dinámicas o estáticas. Una asociación de seguridad establecida puede ser un certificado dependiente del tiempo, con una vida predeterminada (p. ej., una semana, un mes, un año), requiriendo así una nueva ratificación después de la caducidad de la validez del certificado. Una asociación de seguridad estática es verificada cuando se establece. Una asociación de seguridad dinámica es creada con un cliente itinerante que tiene una nueva pasarela de acceso móvil. Si no hay ningún usuario itinerante entre la MAG y el concentrador (o la LMA), tampoco se necesita ningún túnel de IPSec entre ellos. El primer terminal que es autenticado mediante la MAG ante la red y que necesita la conexión en cuestión comienza una creación dinámica de SA entre la MAG y el concentrador adecuado (o la LMA).

Debería observarse que la red de interconexión, la red de origen y / o la red de itinerancia, en la práctica, pueden

pertenecer a la misma compañía, pero son consideradas lógicamente como operadores distintos desde el punto de vista de la presente solución.

Los elementos y etapas mostrados en las figuras están simplificados y solamente intentan describir la idea de la invención. Otros elementos pueden ser usados y / u otras funciones pueden ser llevadas a cabo entre las etapas. Los elementos sirven solamente como ejemplos y pueden contener solamente algo de la información mencionada anteriormente. Los elementos también pueden incluir otra información, y los títulos pueden apartarse de los dados anteriormente. El orden de los elementos y / o etapas puede apartarse del dado. En lugar de, o además de, un nodo ancla, un nodo concentrador, un nodo de acceso y / o un terminal de usuario, las operaciones descritas anteriormente pueden ser realizadas en cualquier otro elemento de un sistema de comunicaciones.

Además de los medios de la técnica anterior, un sistema, o los nodos de red de un sistema, que implementan la funcionalidad de la invención comprenden medios para establecer una asociación de seguridad y para transmitir datos utilizando la asociación de seguridad establecida, de la manera descrita anteriormente. Los nodos de red y los terminales de usuario existentes comprenden procesadores y memoria que pueden ser utilizados en las operaciones de la invención. Todos los cambios necesarios en la implementación de la invención pueden ser llevados a cabo usando suplementos o actualizaciones de rutinas de software y / o de rutinas incluidas en circuitos integrados específicos de la aplicación (ASIC) y / o circuitos programables, tales como los EPLD (dispositivos lógicos eléctricamente programables) o las FPGA (formaciones de compuertas programables en el terreno).

Será obvio para una persona experta en la técnica que, según avanza la tecnología, el concepto inventivo puede ser implementado de diversas maneras. La invención y sus realizaciones no están limitadas a los ejemplos descritos anteriormente, sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para proporcionar un servicio de seguridad al tráfico de datos en un sistema (S) de comunicaciones que implementa el protocolo IPv6 móvil delegado, comprendiendo el sistema (S)

una red (N1) del operador de origen,

una red (N2, N3, N4) del operador de itinerancia,

una red (GRXa, GRXb) del operador de interconexión, y

uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario,

comprendiendo el procedimiento establecer al menos una asociación de seguridad de IPsec, específica del operador, para asegurar el tráfico de datos en el sistema (S),

caracterizado porque el procedimiento comprende

establecer una primera asociación (SA1) de seguridad individual entre un nodo ancla (LMA1) situado en la red (N1) del operador de origen y un nodo concentrador (Ha, Hb) situado en la red (GRXa, GRXb) del operador de interconexión, en donde el nodo concentrador (Ha, Hb) es un nodo delegado;

establecer una segunda asociación (SA2, SA3, SA4) de seguridad individual entre un nodo (MAG2, MAG3) de acceso situado en la red (N2, N3, N4) del operador de itinerancia y el nodo concentrador (Ha, Hb) situado en la red (GRXa, GRXb) del operador de interconexión; y

transmitir tráfico de datos entre el nodo ancla (LMA1) situado en la red (N1) del operador de origen y dichos uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario itinerantes en la red (N2, N3, N4) del operador de itinerancia, de modo que el tráfico de datos transmitido entre el nodo ancla (LMA1) y el nodo concentrador (Ha, Hb) sea asegurado usando la primera asociación (SA1) de seguridad individual, y el tráfico de datos transmitido entre el nodo (MAG2, MAG3) de acceso y el nodo concentrador (Ha, Hb) sea asegurado usando la respectiva segunda asociación (SA2, SA3, SA4) de seguridad individual, en donde la red (N1) del operador de origen es la red de origen de dichos uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario que están representados por la misma primera asociación (SA1) de seguridad individual entre el nodo concentrador (Ha, Hb) y el nodo ancla (LMA1).

2. Un procedimiento según la reivindicación 1, **caracterizado porque** la primera asociación (SA1) de seguridad individual es específica para la red (N1) del operador de origen.

3. Un procedimiento según la reivindicación 1 o 2, **caracterizado porque** la segunda asociación (SA2, SA3, SA4) de seguridad individual es específica para la red (N1) del operador de origen y la red (N2, N3, N4) del operador de itinerancia.

4. Un procedimiento según la reivindicación 1, 2 o 3, **caracterizado por** establecer una asociación (SA2, SA3, SA4) de seguridad entre la red (N1) del operador de origen y cada red (N2, N3, N4) de itinerancia asociada de la red (N1) del operador de origen.

5. Un procedimiento según cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** la primera asociación (SA1) de seguridad individual caduca después de un periodo de tiempo predeterminado.

6. Un procedimiento según cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** la segunda asociación (SA2, SA3, SA4) de seguridad caduca después de un periodo de tiempo predeterminado.

7. Un procedimiento según cualquiera de las reivindicaciones 1 a 6, **caracterizado por** utilizar un protocolo IPv6 móvil delegado entre la red del operador de interconexión y la red del operador de origen, y entre la red del operador de interconexión y la red del operador de itinerancia.

8. Un sistema (S) de comunicaciones que implementa el protocolo IPv6 móvil delegado y que está adaptado para proporcionar un servicio de seguridad al tráfico de datos, comprendiendo el sistema (S)

una red (N1) del operador de origen,

una red (N2, N3, N4) del operador de itinerancia,

una red (GRXa, GRXb) del operador de interconexión, y

uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario,

estando el sistema (S) dispuesto para establecer al menos una asociación de seguridad de IPsec específica del operador, para asegurar el tráfico de datos,

caracterizado porque el sistema (S) está dispuesto para

establecer una primera asociación (SA1) de seguridad individual entre un nodo ancla (LMA1) situado en la red (N1) del operador de origen y un nodo concentrador (Ha, Hb) situado en la red (GRXa, GRXb) del operador de interconexión, en donde el nodo concentrador (Ha, Hb) es un nodo delegado;

establecer una segunda asociación (SA2, SA3, SA4) de seguridad individual entre un nodo (MAG2, MAG3) de acceso situado en la red (N2, N3, N4) del operador de itinerancia y el nodo concentrador (Ha, Hb) situado en la red (GRXa, GRXb) del operador de interconexión; y

transmitir el tráfico de datos entre el nodo ancla (LMA1) situado en la red (N1) del operador de origen y dichos uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario en itinerancia en la red (N2, N3, N4) del operador de itinerancia, de modo que el tráfico de datos transmitido entre el nodo ancla (LMA1) y el nodo concentrador (Ha, Hb) sea asegurado usando la primera asociación (SA1) de seguridad individual, y el tráfico de datos transmitido entre el nodo (MAG2, MAG3) de acceso y el nodo concentrador (Ha, Hb) sea asegurado usando la respectiva segunda asociación (SA2, SA3, SA4) de seguridad individual, en donde la red (N1) del operador de origen es la red de origen de dichos uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario, que están representados por la misma primera asociación (SA1) de seguridad individual entre el nodo concentrador (Ha, Hb) y el nodo ancla (LMA1).

9. Un sistema según la reivindicación 8, **caracterizado porque** la primera asociación (SA1) de seguridad individual es específica para la red (N1) del operador de origen; y

la segunda asociación (SA2, SA3, SA4) de seguridad individual es específica para la red (N1) del operador de origen y la red (N2, N3, N4) del operador de itinerancia.

10. Un nodo concentrador (Ha, Hb) para un sistema (S) de comunicaciones que implementa el protocolo IPv6 móvil delegado, y que está adaptado para proporcionar un servicio de seguridad al tráfico de datos y establecer al menos una asociación de seguridad de IPsec, específica del operador, para asegurar el tráfico de datos, en donde el nodo concentrador (Ha, Hb) está situado en una red (GRXa, GRXb) del operador de interconexión, **caracterizado porque** el nodo concentrador (Ha, Hb) es un nodo delegado dispuesto para

establecer una primera asociación (SA1) de seguridad individual para el tráfico de datos asegurado con un nodo ancla (LMA) situado en una red (N1) del operador de origen;

establecer una segunda asociación (SA2, SA3, SA4) de seguridad individual para el tráfico de datos asegurado con un nodo (MAG2, MAG3) de acceso situado en una red (N2, N3, N4) del operador de itinerancia; y

transmitir el tráfico de datos entre el nodo ancla (LMA1) situado en la red (N1) del operador de origen y uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario en itinerancia en la red (N2, N3, N4) del operador de itinerancia, de modo que el tráfico de datos transmitido entre el nodo ancla (LMA1) y el nodo concentrador (Ha, Hb) sea asegurado usando la primera asociación (SA1) de seguridad individual, y el tráfico de datos transmitido entre el nodo (MAG2, MAG3) de acceso y el nodo concentrador (Ha, Hb) sea asegurado usando la respectiva segunda asociación (SA2, SA3, SA4) de seguridad individual, en donde la red (N1) del operador de origen es la red de origen de dichos uno o más terminales (UE1-2, UE1-3, UE1-4) de usuario que están representados por la misma primera asociación (SA1) de seguridad individual entre el nodo concentrador (Ha, Hb) y el nodo ancla (LMA1).

11. Un nodo concentrador (Ha, Hb) según la reivindicación 10, **caracterizado porque** la primera asociación (SA1) de seguridad individual es específica para la red (N1) del operador de origen.

12. Un nodo concentrador (Ha, Hb) según la reivindicación 10 u 11, **caracterizado porque** la segunda asociación (SA2, SA3, SA4) de seguridad individual es específica para la red (N1) del operador de origen y la red (N2, N3, N4) del operador de itinerancia.

13. Un nodo concentrador (Ha, Hb) según la reivindicación 10, 11 o 12, **caracterizado porque** la primera asociación (SA1) de seguridad individual caduca después de un periodo de tiempo predeterminado.

14. Un nodo concentrador (Ha, Hb) según cualquiera de las reivindicaciones 10 a 13, **caracterizado porque** la segunda asociación (SA2, SA3, SA4) de seguridad individual caduca después de un periodo de tiempo predeterminado.

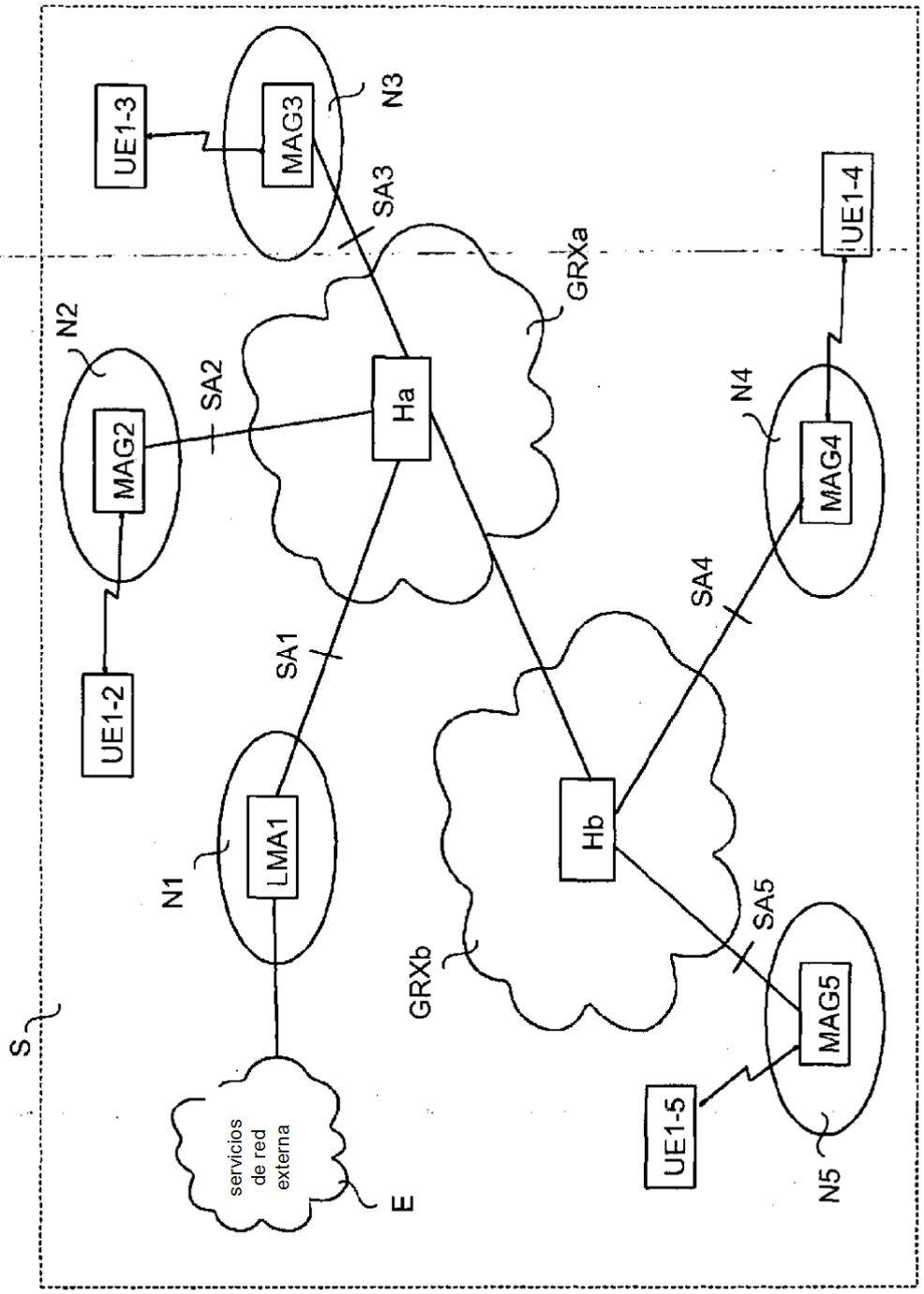
S
UE1-3
MAG3
N3
SA3
GRXa
N2
MAG2
SA2
Ha
UE1-4
N4
MAG4
UE1-2
SA1
SA4
N1
LMA1
Hb
GRXb
SA5
MAG5
UE1-5
N5
servicios de red externa
E

Fig. 1

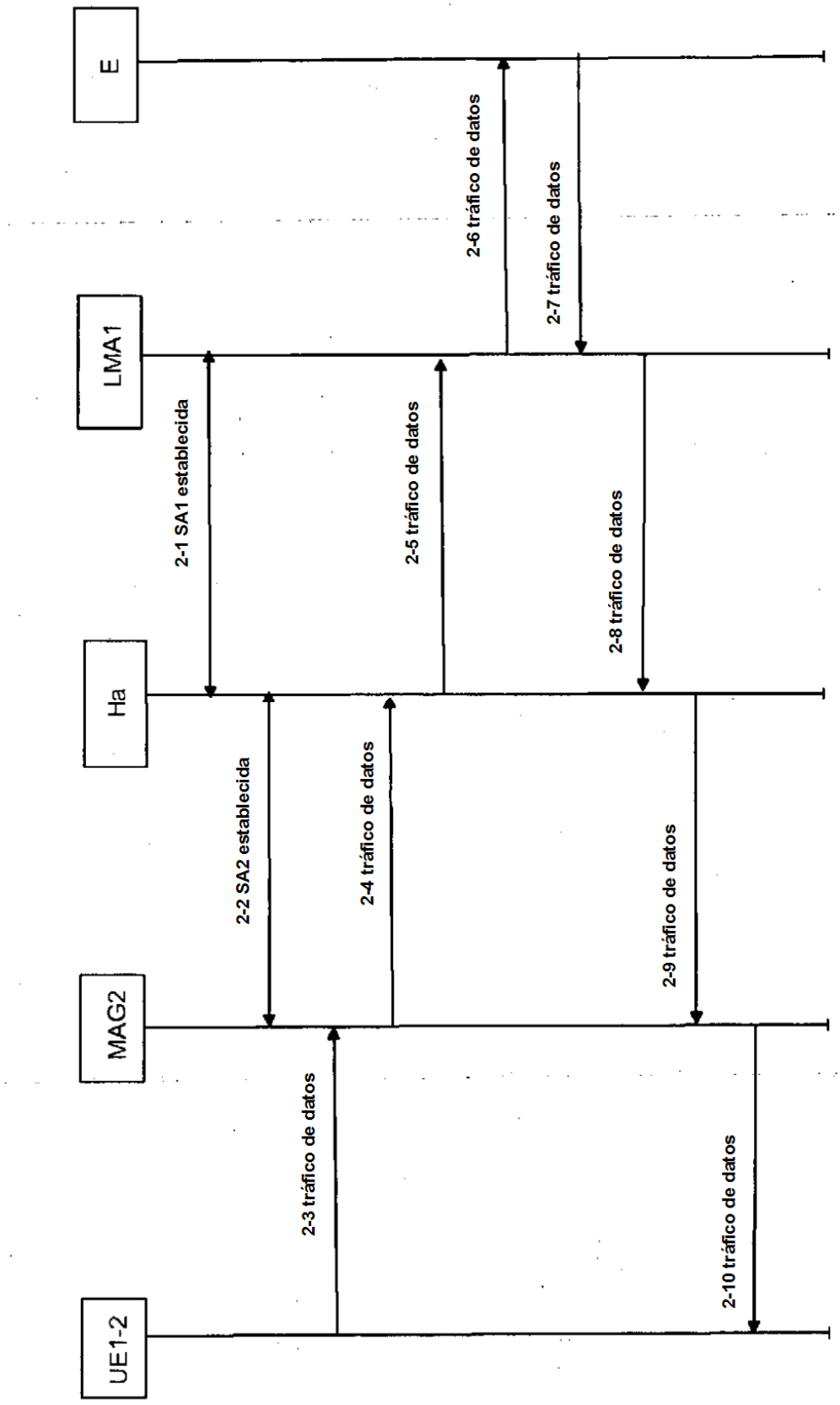
E
LMA1
Ha
MAG2
UE1-2
2-1 SA1 establecida
2-2 SA2 establecida
2-3 tráfico de datos
2-4 tráfico de datos
2-5 tráfico de datos
2-6 tráfico de datos
2-7 tráfico de datos
2-8 tráfico de datos
2-9 tráfico de datos
2-10 tráfico de datos

Fig. 2

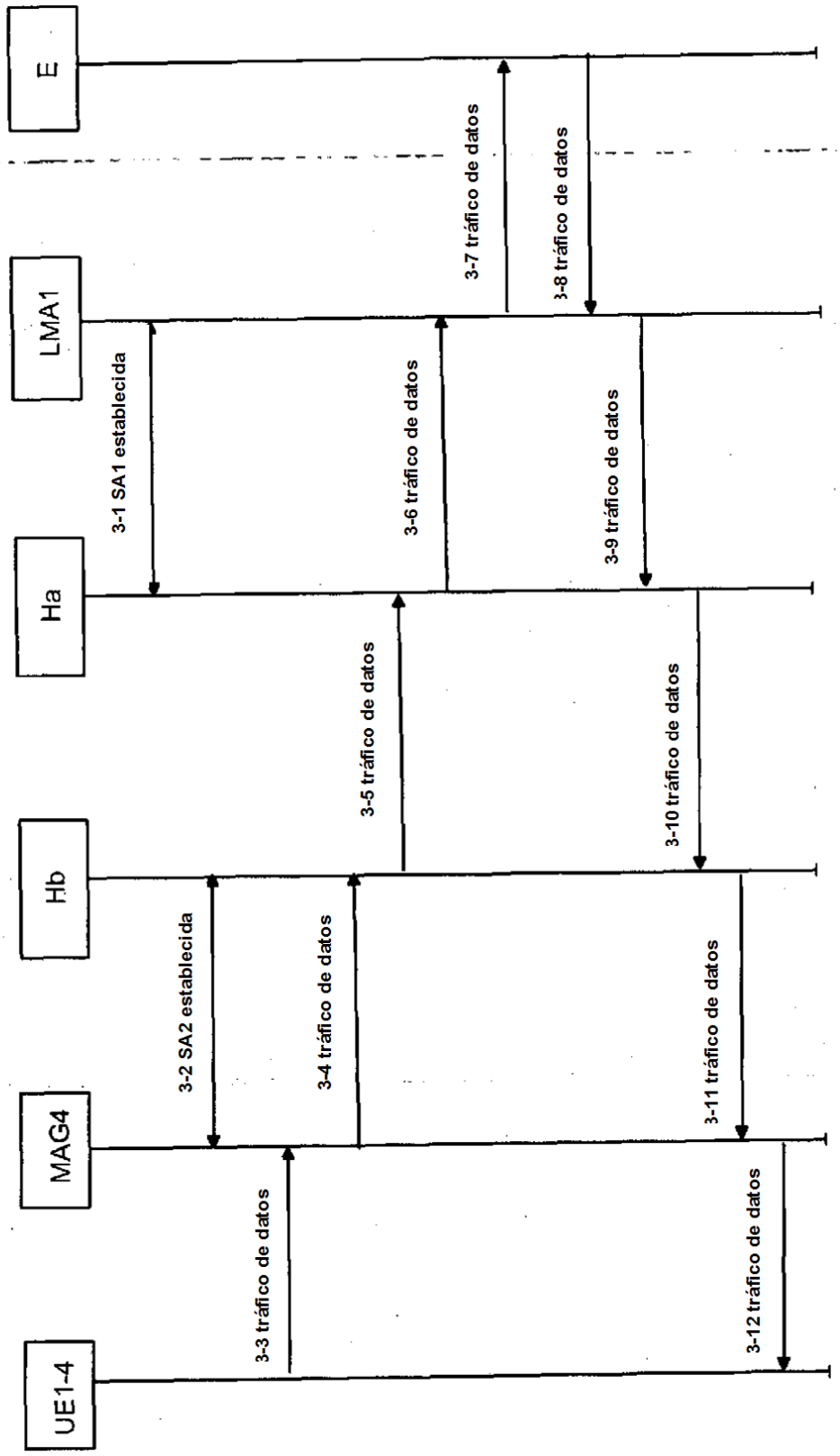
E
LMA1
Ha
Hb
MAG4
UE1-4
3-1 SA1 establecida
3-2 SA2 establecida
3-3 tráfico de datos
3-4 tráfico de datos
3-5 tráfico de datos
3-6 tráfico de datos
3-7 tráfico de datos
3-8 tráfico de datos
3-9 tráfico de datos
3-10 tráfico de datos
3-11 tráfico de datos
3-12 tráfico de datos

Fig. 3

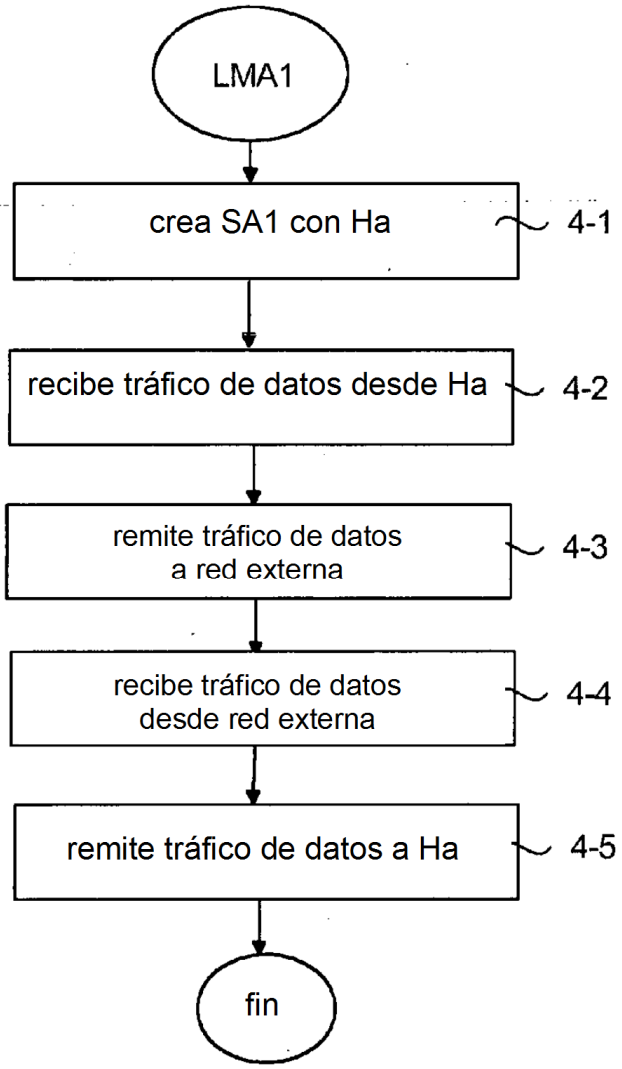
LMA1
crea SA1 con Ha
4-1
recibe tráfico de datos desde Ha
4-2
remite tráfico de datos a red externa
4-3
recibe tráfico de datos desde red externa
4-4
remite tráfico de datos a Ha
4-5
fin

Fig. 4

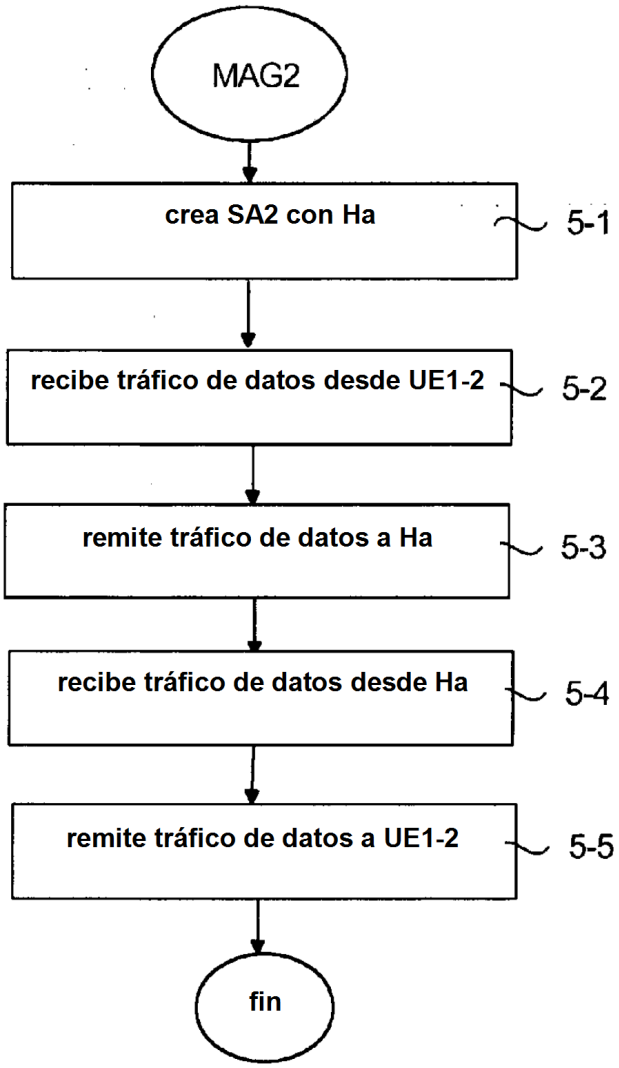
MAG2
crea SA2 con Ha
5-1
recibe tráfico de datos desde UE1-2
5-2
remite tráfico de datos a Ha
5-3
recibe tráfico de datos desde Ha
5-4
remite tráfico de datos a UE1-2
5-5
fin

Fig. 5

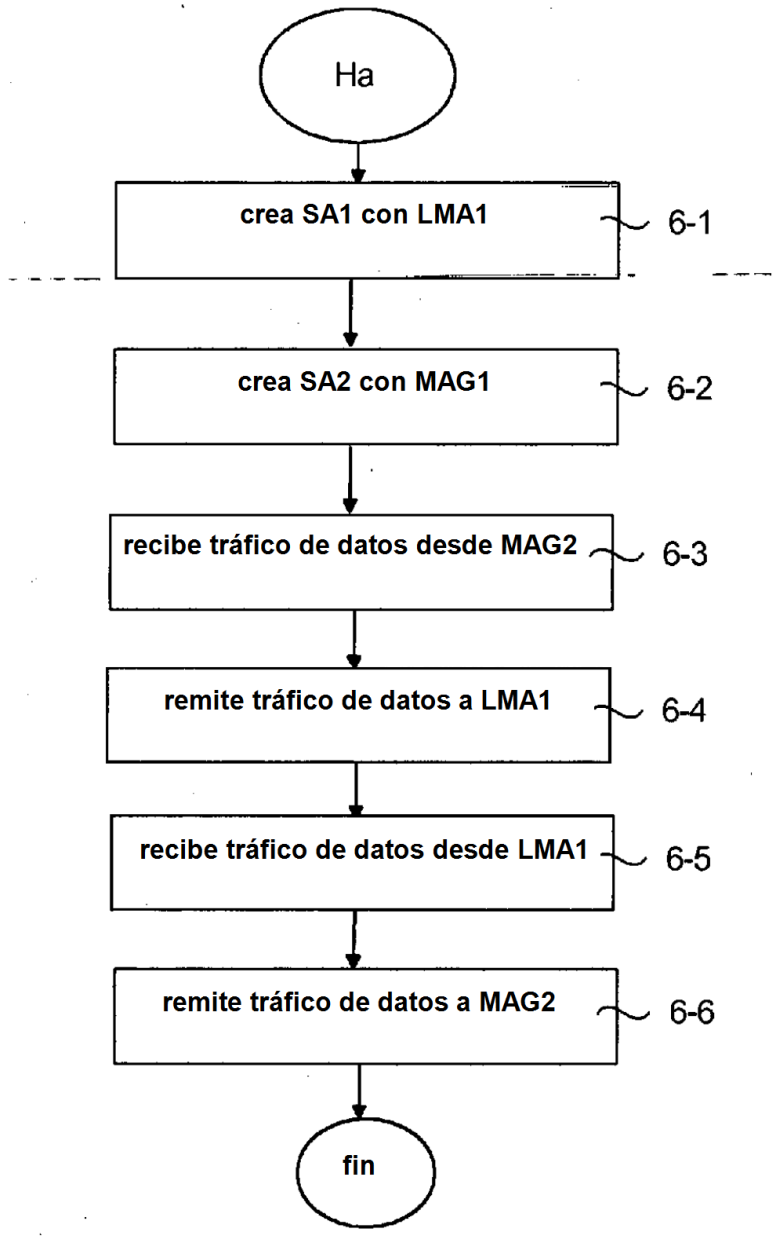
Ha
crea SA1 con LMA1
6-1
crea SA2 con MAG1
6-2
recibe tráfico de datos desde MAG2
6-3
remite tráfico de datos a LMA1
6-4
recibe tráfico de datos desde LMA1
6-5
remite tráfico de datos a MAG2
6-6
fin

Fig. 6

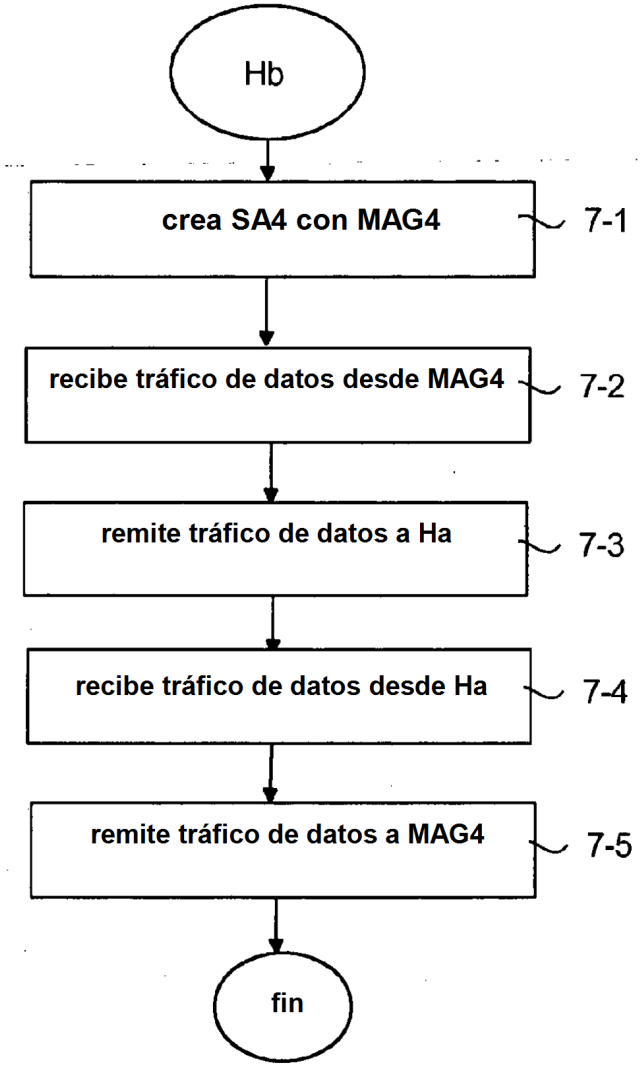
Hb
crea SA4 con MAG4
7-1
recibe tráfico de datos desde MAG4
7-2
remite tráfico de datos a Ha
7-3
recibe tráfico de datos desde Ha
7-4
remite tráfico de datos a MAG4
7-5
fin

Fig. 7