(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 670 853**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 80/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.03.2008 PCT/US2008/057280**

(87) Fecha y número de publicación internacional: **09.10.2008 WO08121544**

(96) Fecha de presentación y número de la solicitud europea: **17.03.2008 E 08732376 (2)**

(97) Fecha y número de publicación de la concesión europea: **18.04.2018 EP 2137925**

(54) Título: **Perfil de usuario, política y distribución de claves de PMIP en una red de comunicación inalámbrica**

(30) Prioridad:

16.03.2007 US 895298 P
14.03.2008 US 48883

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.06.2018

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
ATTN: INTERNATIONAL IP ADMINISTRATION,
5775 MOREHOUSE DRIVE
SAN DIEGO, CA 92121, US

(72) Inventor/es:

WANG, JUN;
MAHENDRAN, ARUNGUNDRAM C. y
NARAYANAN, VIDYA

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Perfil de usuario, política y distribución de claves de PMIP en una red de comunicación inalámbrica

ANTECEDENTES

Reivindicación de prioridad en virtud del artículo 35 U.S.C. §119

[0001] La presente solicitud de patente reivindica prioridad de la solicitud provisional de EE. UU. n.º 60/895.298 titulada "3GPP2 Network Evolution: User Profile Policy, and PMIP Key" [Evolución de la red 3GPP2: Política de perfil de usuario, y clave de PMIP] presentada el 16 de marzo de 2007, y otorgada al cesionario de la presente y por la presente incorporada expresamente por referencia en el presente documento.

Campo

[0002] Al menos una característica se refiere a sistemas de comunicación y, más particularmente, a un procedimiento para facilitar la distribución segura de información de dispositivos móviles dentro de una red inalámbrica, tal como una red de banda ancha ultra móvil (UMB).

Antecedentes

[0003] En la evolución de diversas redes de comunicación inalámbrica dentro de 3GPP2, un tipo de arquitectura de red se conoce como una red de banda ancha ultra móvil (UMB) y está destinada a mejorar el estándar de telefonía móvil CDMA2000 para aplicaciones y requisitos de próxima generación. Las redes de datos en paquetes UMB se basan en tecnologías de red de Internet (TCP/IP) que se ejecutan en un sistema de radio de próxima generación y está destinada para ser más eficiente y capaz de proporcionar más servicios que las tecnologías a las que reemplaza. UMB está destinada a ser una tecnología de cuarta generación (4G) y usa una red TCP/IP subyacente de baja latencia, de alto ancho de banda con servicios de alto nivel tales como voz integrada. La cantidad mucho mayor de ancho de banda (en comparación con las generaciones previas), y las latencias mucho más bajas, posibilitan el uso de diversos tipos de aplicaciones que previamente eran imposibles, en tanto que continúan ofreciendo servicios de voz de alta calidad (o de más alta calidad).

[0004] Las redes UBM tienen una gestión menos centralizada de sus nodos de acceso a red, conocidos como estaciones base evolucionadas (eBS). Por ejemplo, dichos nodos de acceso pueden realizar muchas de las mismas funciones que la estación base (BS) y el controlador de estación base (BSC) en una red CDMA. Debido a esta arquitectura de red más distributiva, se producen varios problemas al tratar de mantener seguro un identificador de acceso a red (NAI) de un terminal de acceso (AT).

[0005] En algunas arquitecturas de red de la técnica anterior, el NAI (o su identificador de terminal de acceso equivalente) se transmite por el terminal de acceso por vía aérea al nodo servidor de datos en paquetes (PDSN), que lo usa para la autenticación, informe de contabilidad, y/o funciones de recuperación de políticas. Al transmitir el NAI por vía aérea, lo hace susceptible a espionaje e inseguro.

[0006] En una red UMB, el NAI no se envía por vía aérea. En cambio, dependiendo de los procedimientos de protocolo de autenticación extensible (EAP), el autentificador puede no conocer el NAI de un terminal de acceso. Esto se puede denominar NAI anónimo. Sin embargo, se produce un problema en cómo autenticar un AT en tanto que se implementa el NAI anónimo.

[0007] En una red UMB, el perfil de usuario, y el perfil de usuario de calidad de servicio (QoS) se envía al controlador de red de referencia de sesión (SRNC) desde la autenticación, autorización y contabilidad local y doméstica (LAAA/HAAA) a través de autenticación de acceso satisfactoria. Sin embargo, es necesario también que el perfil de usuario se envíe a una pasarela de acceso (AGW) (por ejemplo, a través de autorización de servicios IP). Por lo tanto, existe un problema sobre cómo enviar el perfil de usuario a una AGW en tanto que se implementa el NAI anónimo.

[0008] Si se usa un túnel de PMIPv4 entre una eBS y una AGW dentro de una red UMB, es necesario que la clave de MN-HA (por ejemplo, puede ser por clave basada en AT o por clave de par eBS-AGW) se envíe a tanto la eBS como la AGW. De este modo, se produce un problema sobre cómo enviar la clave de MN-HA usada para el túnel de PMIPv4 entre la eBS y la AGW al SRNC y a la AGW.

[0009] En consecuencia, se necesita una manera de abordar estos problemas cuando se implementa el NAI anónimo dentro de una red UMB.

[0010] Además se llama la atención sobre el documento MADJID NAKHJIRI NARAYANAN VENKITARAMAN MOTOROLA LABS: "EAP based Proxy Mobile IP key bootstrapping: A WiMAX applicability example; draft-nakhjiri-pmip-key-02.txt" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, n. ° 2,

01-02-2006, que describe un servidor de AAA que deriva una clave de PMIP y transporta la clave al PMN junto con la autenticación de la red de acceso EAP. De modo que el PMN puede generar solicitudes de registro (RRQ) de IP móvil autenticadas hacia el HA usando la clave de PMIP como clave de autenticación de mensaje.

SUMARIO

[0011] De acuerdo con la presente invención, se proporciona un procedimiento como se expone en la reivindicación 1, un aparato como se expone en la reivindicación 9, un procedimiento como se expone en la reivindicación 10, un aparato como se expone en la reivindicación 11, un procedimiento como se expone en la reivindicación 13 y un aparato como se expone en la reivindicación 14. Modos de realización adicionales de la invención se reivindican en las reivindicaciones dependientes.

[0012] Se proporciona un procedimiento de funcionamiento en un servidor de autenticación para una red de comunicación inalámbrica para asegurar una clave de usuario primario. Se recibe una solicitud de autenticación de acceso desde un par de autenticación inalámbrico. Se genera un identificador de usuario secundario, en el que se asocia la clave de usuario secundario con un identificador de usuario primario para el par de autenticación inalámbrico. El identificador de usuario secundario es el proporcionado a un autentificador asociado con el par de autenticación. La información de perfil de usuario se puede recuperar en función del identificador de usuario primario. La información de perfil de usuario se puede enviar al autentificador.

[0013] La red de comunicación puede incluir al menos una entre una red compatible con banda ancha ultra móvil (UMB), una red compatible con WiMAX o una red compatible con evolución a largo plazo (LTE). El servidor de autenticación puede ser una entidad de autenticación, autorización y contabilidad (AAA), y el par de autenticación es un terminal de acceso (AT) inalámbrico. El autentificador puede ser un controlador de red de referencia de sesión (SRNC) asociado con una estación base (BS) que presta servicio al terminal de acceso inalámbrico (AT) en una red compatible de banda ancha ultra móvil (UMB) y el identificador de usuario primario es un identificador de acceso a red (NAI) para el terminal de acceso inalámbrico. La estación base servidora puede estar ubicada con el controlador de red de referencia de sesión (SRNC).

[0014] El identificador de usuario secundario puede ser un número generado aleatoriamente que posteriormente se asocia con el identificador de usuario primario. El identificador de usuario secundario también puede ser el identificador de usuario primario. El identificador de usuario secundario puede ser una función del identificador de usuario primario.

[0015] Se proporciona un servidor de autenticación que incluye un circuito de procesamiento adaptado para: (a) recibir una solicitud de autenticación de acceso desde un par de autenticación inalámbrico; (b) generar un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico; (c) proporcionar el identificador de usuario secundario a un autentificador asociado con el par de autenticación; (d) recuperar información de perfil de usuario en función del identificador de usuario primario; (e) proporcionar la información de perfil de usuario al autentificador.

[0016] El servidor de autenticación puede comprender además una interfaz de comunicación adaptada para comunicarse por al menos una entre una red compatible con banda ancha ultra móvil (UMB), una red compatible con WiMAX o una red compatible con evolución a largo plazo (LTE). El servidor de autenticación puede ser una entidad de autenticación, autorización y contabilidad (AAA), y el par de autenticación es un terminal de acceso (AT) inalámbrico. El autentificador puede ser un controlador de red de referencia de sesión (SRNC) asociado con una estación base (BS) que presta servicio al terminal de acceso inalámbrico (AT) en una red compatible de banda ancha ultra móvil (UMB) y el identificador de usuario primario es un identificador de acceso a red (NAI) para el terminal de acceso inalámbrico. El identificador de usuario secundario puede ser (a) un número generado aleatoriamente que se asocia posteriormente con el identificador de usuario primario, (b) el identificador de usuario primario, y/o (c) una función del identificador de usuario primario.

[0017] En consecuencia, también se proporciona un servidor de autenticación que comprende: (a) un medio para recibir una solicitud de autenticación de acceso desde un par de autenticación inalámbrico; (b) un medio para generar un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico; (c) un medio para proporcionar el identificador de usuario secundario a un autentificador asociado con el par de autenticación; (d) un medio para recuperar información de perfil de usuario en función del identificador de usuario primario; y/o (e) un medio para proporcionar la información de perfil de usuario al autentificador.

[0018] También se proporciona un programa informático de funcionamiento en un servidor de autenticación para asegurar un identificador de usuario primario, que cuando se ejecuta por un procesador provoca que el procesador: (a) reciba una solicitud de autenticación de acceso desde un par de autenticación inalámbrico; (b) genere un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico; (c) proporcione el identificador de usuario secundario a un autentificador asociado con el par de

autenticación; (d) recupere información de perfil de usuario en función del identificador de usuario primario; y/o (e) proporcione la información de perfil de usuario al autentificador.

[0019] También se proporciona un procedimiento por un servidor de autenticación para distribuir el perfil de usuario y/o la información de políticas dentro de una red de comunicación. Se autentica un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red. La información de perfil de usuario asociada con el par de autenticación se recupera y envía a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación. La información de perfil de usuario también se envía a un autentificador que facilita las comunicaciones para el par de autenticación. El servidor de autenticación puede ser una entidad de autenticación, autorización y contabilidad (AAA) que es parte de la red de comunicación.

[0020] En un ejemplo, el envío de la información de perfil de usuario al nodo de pasarela de red puede incluir hacer que un autentificador para la red de comunicación envíe la información de perfil de usuario al nodo de pasarela de red. En otro ejemplo, el envío de la información de perfil de usuario al nodo de pasarela de red incluye hacer que el servidor de autenticación envíe la información de perfil de usuario al nodo de pasarela de red. La información de perfil de usuario puede incluir al menos uno entre un perfil de usuario, la política de usuario, la calidad de servicio para el perfil de usuario, para servicios de comunicación del par de autenticación.

[0021] Adicionalmente, el procedimiento puede comprender además: (a) enviar una solicitud de políticas desde el nodo de pasarela de red a una entidad de función de recursos y control de políticas (PCRF); (b) enviar una solicitud de identificador de usuario primario desde la entidad PCRF al servidor de autenticación, en la que el identificador de usuario primario está asociado exclusivamente con el par de autenticación; (c) enviar una respuesta desde el servidor de autenticación a la entidad PCRF que incluye el identificador de usuario primario solicitado; (d) obtener una política de usuario en la entidad PCRF para el par de autenticación que usa el identificador de usuario primario; y/o (e) enviar la política de usuario desde la entidad PCRF al nodo de pasarela de red.

[0022] El autentificador puede ser un controlador de red de referencia de sesión (SRNC) asociado con una estación base que presta servicio al par de autenticación en una red compatible de banda ancha ultra móvil (UMB), y el identificador confidencial es un identificador de acceso a red para el terminal de acceso inalámbrico.

[0023] También se proporciona un servidor de autenticación que incluye un circuito de procesamiento adaptado para: (a) autenticar un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red; (b) recuperar la información de perfil de usuario asociada con el par de autenticación; (c) enviar la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación; (d) enviar la información de perfil de usuario a un autentificador que facilite las comunicaciones para el par de autenticación; (e) recibir una solicitud de identificador de usuario primario de una entidad PCRF, en la que se asocia exclusivamente el identificador de usuario primario con el par de autenticación; y/o (f) enviar una respuesta a la entidad PCRF que incluya el identificador de usuario primario solicitado.

[0024] En consecuencia, se proporciona un servidor de autenticación que comprende: (a) un medio para autenticar un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red; (b) un medio para recuperar información de perfil de usuario asociada con el par de autenticación; (c) un medio para enviar la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación; (d) un medio para enviar la información de perfil de usuario a un autentificador que facilite las comunicaciones para el par de autenticación; (e) un medio para recibir una solicitud de identificador de usuario primario desde una entidad PCRF, en el que el identificador de usuario primario está asociado exclusivamente con el par de autenticación; y/o (f) un medio para enviar una respuesta a la entidad PCRF que incluya el identificador de usuario primario solicitado.

[0025] También se proporciona un programa informático de funcionamiento en un servidor de autenticación para proporcionar información de usuario, que cuando se ejecuta por un procesador provoca que el procesador: (a) autentique un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red; (b) recupere información de perfil de usuario asociada con el par de autenticación; (c) envíe la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación; (d) envíe la información de perfil de usuario a un autentificador que facilita las comunicaciones para el par de autenticación; (e) reciba una solicitud de identificador de usuario primario de una entidad PCRF, en la que se asocia exclusivamente el identificador de usuario primario con el par de autenticación; y/o (f) envíe una respuesta a la entidad PCRF que incluya el identificador de usuario primario solicitado.

[0026] Se proporciona un procedimiento de funcionamiento en una red de comunicación. Se proporciona la conectividad de red inalámbrica a un par de autenticación a través de un primer nodo de acceso a red. Se proporciona una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y un nodo de red PMIP usado para proporcionar comunicaciones al par de autenticación. La clave de PMIP se proporciona entonces a un primer autentificador asociado al primer nodo de acceso a red. Las comunicaciones se pueden encaminar al primer nodo de acceso a red.

[0027] Posteriormente, se puede recibir una solicitud en el nodo de red de PMIP desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación. El nodo de red de PMIP puede verificar si la entidad solicitante conoce la clave de PMIP. En un ejemplo, las comunicaciones se pueden reencaminar a un segundo nodo de acceso a red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. En otro ejemplo, se pueden reencaminar las comunicaciones a un segundo nodo de pasarela de red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. El reencaminamiento de las comunicaciones puede incluir el establecimiento de un nuevo túnel de IP móvil de proxy entre el primer nodo de red de PMIP y una nueva entidad de red servidora. En un ejemplo, se puede generar la clave de PMIP en una entidad de autenticación, autorización y contabilidad (AAA) o un nodo de pasarela de red. El nodo de red de PMIP puede ser un nodo de pasarela de red.

[0028] También se proporciona un nodo de red de PMIP que incluye un circuito de procesamiento adaptado para: (a) proporcionar conectividad de red inalámbrica a un par de autenticación a través de un primer nodo de acceso a red; (b) proporcionar una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y el nodo de red de PMIP usado para proporcionar comunicaciones al par de autenticación; (c) proporcionar la clave de PMIP a un primer autentificador asociado al primer nodo de acceso a red; (d) recibir una solicitud desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación; (e) verificar si la entidad solicitante conoce la clave de PMIP; (f) reencaminar las comunicaciones a un segundo nodo de acceso a red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP; y/o (g) reencaminar las comunicaciones a un segundo nodo de pasarela de red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. El reencaminamiento de comunicaciones puede incluir el establecimiento de un nuevo túnel de IP móvil de proxy entre el primer nodo de red de PMIP y una nueva entidad de red servidora.

[0029] En consecuencia, también se proporciona un nodo de red de PMIP, que comprende: (a) un medio para proporcionar conectividad de red inalámbrica a un par de autenticación a través de un primer nodo de acceso a red; (b) un medio para proporcionar una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y el nodo de red de PMIP usado para proporcionar comunicaciones al par de autenticación; (c) un medio para proporcionar la clave de PMIP a un primer autentificador asociado al primer nodo de acceso a red; recibir una solicitud desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación; (d) un medio para verificar si una entidad solicitante conoce la clave de PMIP; (e) un medio para reencaminar las comunicaciones a un segundo nodo de acceso a red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP; y/o (f) un medio para reencaminar las comunicaciones a un segundo nodo de pasarela de red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. El reencaminamiento de comunicaciones puede incluir el establecimiento de un nuevo túnel de IP móvil de proxy entre el primer nodo de red de PMIP y una nueva entidad de red servidora.

[0030] También se proporciona un programa informático en funcionamiento en un nodo de red de PMIP, que cuando se ejecuta por un procesador provoca que el procesador: (a) proporcione conectividad de red inalámbrica a un par de autenticación a través de un primer nodo de acceso a red; (b) proporcione una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y el nodo de red de PMIP usado para proporcionar las comunicaciones al par de autenticación; (c) proporcione la clave de PMIP a un primer autentificador asociado al primer nodo de acceso a red; (d) reciba una solicitud desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación; (e) verifique si la entidad solicitante conoce la clave de PMIP; (f) reencamine las comunicaciones a un segundo nodo de acceso a red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP; y/o (g) reencamine las comunicaciones a un segundo nodo de pasarela de red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0031] Diversas características, la naturaleza y las ventajas pueden resultar evidentes a partir de la descripción detallada expuesta a continuación cuando se considera conjuntamente con los dibujos, en los que los mismos caracteres de referencia se identifican de manera correspondiente en toda su extensión.

La figura 1 es un diagrama de bloques de una red UMB en el que se pueden implementar una o más características de NAI seguro, perfil de usuario seguro y distribución de políticas, y/o distribución de claves PMIP de acuerdo con un ejemplo.

La figura 2 es un diagrama de flujo que ilustra un procedimiento de autenticación mediante el cual un identificador de acceso a red (NAI) no se transmite por aire durante una autenticación de acceso a red entre un terminal de acceso (AT) y una entidad de autenticación, autorización y contabilidad doméstica (HAAA).

La figura 3 ilustra un procedimiento de funcionamiento en un servidor de autenticación (por ejemplo, HAAA) para una red de comunicación inalámbrica que se proporciona para asegurar una clave de usuario primario.

La figura 4 es un diagrama de bloques que ilustra cómo se puede proporcionar el servicio inalámbrico a un AT a medida que se desplaza desde una primera eBS a una segunda eBS en una red UMB.

La figura 5 ilustra cómo una AGW puede recuperar el perfil de usuario a partir de una LAAA cuando se establece un nuevo túnel de PMIP y solicitar la política de usuario desde la PCRF en una configuración de SRNC distribuida.

La figura 6 ilustra cómo una AGW puede recuperar el perfil de usuario a partir de una LAAA cuando se establece un nuevo túnel de PMIP y solicitar la política de usuario desde la PCRF en una configuración de SRNC centralizada.

La figura 7 ilustra cómo un AGW puede obtener información de perfil de usuario como parte de un proceso de autenticación y política de usuario desde una PCRF en una configuración de SRNC distribuida.

La figura 8 ilustra cómo un AGW puede obtener información de perfil de usuario como parte de un proceso de autenticación y política de usuario desde una PCRF en una configuración de SRNC distribuida.

La figura 9 ilustra cómo una LAAA puede impulsar el perfil de usuario a la AGW y la AGW puede solicitar la política de usuario desde una PCRF en una configuración de SRNC distribuida.

La figura 10 ilustra cómo una LAAA puede impulsar el perfil de usuario a una AGW y la AGW puede solicitar la política de usuario desde una PCRF en una configuración de SRNC centralizada.

La figura 11 ilustra un procedimiento de funcionamiento de un servidor de autenticación para proporcionar un autentificador con información de perfil de usuario.

La figura 12 ilustra un procedimiento para proporcionar un nodo de pasarela de red con información de política de usuario para un par de autenticación de funcionamiento en una red de comunicación.

La figura 13 ilustra un procedimiento para verificar nuevas solicitudes de túnel en una red de comunicación.

La figura 14 ilustra una arquitectura de autenticación encontrada en algunas redes de comunicación.

La figura 15 es un diagrama de bloques que ilustra un servidor de autenticación. El servidor de autenticación puede incluir un circuito de procesamiento 1504 acoplado a una interfaz de comunicación de red.

La figura 16 es un diagrama de bloques que ilustra un ejemplo de un dispositivo de nodo de red de PMIP.

DESCRIPCIÓN DETALLADA

[0032] En la siguiente descripción, se dan detalles específicos para proporcionar una comprensión exhaustiva de las configuraciones. Sin embargo, se entenderá por un experto en la técnica que se pueden llevar a la práctica las configuraciones sin estos detalles específicos. Por ejemplo, se pueden mostrar circuitos en diagramas de bloques a fin de no oscurecer las configuraciones con detalles innecesarios. En otros casos, se pueden mostrar en detalle circuitos, estructuras y técnicas bien conocidos a fin de no oscurecer las configuraciones.

[0033] Además, se debe observar que las configuraciones se pueden describir como un proceso que se representa como un diagrama de flujo, un organigrama, un diagrama estructural o un diagrama de bloques. Aunque un diagrama de flujo puede describir las operaciones como un proceso secuencial, muchas de las operaciones se pueden realizar en paralelo o simultáneamente. Además, el orden de las operaciones se puede reorganizar. Un proceso se termina cuando sus operaciones se completan. Un proceso puede corresponder a un procedimiento, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un proceso se corresponde con una función, su finalización se corresponde con un retorno de la función a la función de llamada o la función principal.

[0034] En uno o más ejemplos y/o configuraciones, las funciones descritas se pueden implementar en hardware, software, firmware o cualquier combinación de los mismos. Si se implementan en software, las funciones, como una o más instrucciones o códigos, se pueden almacenar en, o transmitir por, un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informáticos como medios de comunicación, incluyendo cualquier medio que facilita la transferencia de un programa informático de un lugar a otro. Un medio de almacenamiento puede ser cualquier medio disponible al que se pueda acceder mediante un ordenador de uso general o uso especial. A modo de ejemplo, y no de manera limitativa, dichos medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que se pueda usar para transportar o almacenar medios deseados de código de programa en forma de instrucciones o estructuras de datos y al que se pueda acceder mediante un ordenador de uso general o uso especial o un procesador de uso general o uso especial. Asimismo, cualquier conexión recibe correctamente la denominación de medio legible por ordenador. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota, usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o

tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, el DSL o las tecnologías inalámbricas, tales como infrarrojos, radio y microondas, se incluyen en la definición de medio. Los discos, como se usan en el presente documento, incluyen el disco compacto (CD), el disco de láser, el disco óptico, el disco versátil digital (DVD), el disco flexible y el disco Blu-ray, donde algunos discos normalmente reproducen datos de manera magnética, mientras que otros discos reproducen los datos de manera óptica con láseres. También se incluyen combinaciones de lo anterior dentro del alcance de los medios legibles por ordenador.

[0035] Además, un medio de almacenamiento puede representar uno o más dispositivos para almacenar datos, incluyendo memora de sólo lectura (ROM), memoria de acceso aleatorio (RAM), medios de almacenamiento de disco magnético, medios de almacenamiento óptico, dispositivos de memoria flash y/u otros medios legibles por máquina para almacenar información.

[0036] Además, las configuraciones se pueden implementar mediante hardware, software, firmware, middleware, microcódigo o cualquier combinación de los mismos. Cuando se implementar en software, firmware, middleware o microcódigo, el código de programa o segmentos de código para realizar las tareas necesarias se pueden almacenar en un medio legible por ordenador, tal como un medio de almacenamiento u otro(s) almacenamiento(s). Un procesador puede realizar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o sentencias de programa. Un segmento de código se puede acoplar a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. La información, argumentos, parámetros, datos, etc., se pueden pasar, remitir o transmitir a través de cualquier medio adecuado incluyendo compartición de memoria, paso de mensajes, paso de testigos, transmisión por red, etc.

[0037] En la siguiente descripción, se usa determinada terminología para describir determinadas características. Los términos "terminal de acceso" y "dispositivo de comunicación" se pueden usar indistintamente para referirse a un dispositivo móvil, teléfono móvil, terminal inalámbrico y/u otros tipos de aparatos de comunicación móviles o fijos que se pueden comunicar por una red inalámbrica.

Entorno de red

[0038] Las características descritas en el presente documento se pueden implementar en diversos tipos de redes, incluyendo UMB, WiMAX y redes compatibles con LTE.

[0039] La figura 14 ilustra una arquitectura de autenticación encontrada en algunas redes de comunicación. La red de comunicación 1400 (por ejemplo, una UMB, WiMAX o redes de evolución a largo plazo (LTE)) puede incluir una pluralidad de nodos IP 1404 y 1408 con un par de autenticación 1402, un autentificador 1406 y un servidor de autenticación 1410. Durante el funcionamiento, el par de autenticación 1402 (por ejemplo, el terminal de acceso) se puede autenticar por el autentificador 1406 con la ayuda del servidor de autenticación 1410. En un ejemplo, el autentificador 1406 puede ser un controlador de red de referencia de sesión (SRNC) y el servidor de autenticación 1410 puede ser una entidad de autenticación, autorización y contabilidad doméstica (HAAA). Adicionalmente, los nodos IP 1404 y 1408 pueden incluir una estación base, una pasarela y/u otras entidades de red. Una entidad de políticas 1412 (por ejemplo, PCRF) puede almacenar información de políticas para el par de autenticación 1402.

[0040] En la prestación de servicios de comunicación a un par de autenticación 1402 en la red de comunicación 1400, se necesita un mecanismo o procedimiento para distribuir un perfil de usuario para el par de autenticación 1402 a tanto el autentificador 1406 como el Nodo B de IP (pasarela). Este es particularmente el caso ya que el autentificador 1406 no está ubicado con el Nodo B de IP (pasarela) 1408.

[0041] Adicionalmente, cuando se usa un pseudo-NAI para identificar el par de autenticación 1402 a la red de comunicación, hace que sea difícil distribuir la política de usuario desde una entidad de políticas (por ejemplo, PCRF doméstica) a los nodos de IP 1404 y 1408.

[0042] Adicionalmente, también es problemático generar y distribuir una clave de PMIP entre dos nodos de IP que necesitan configurar un túnel de PMIP. Por ejemplo, en una red UMB, se puede distribuir una clave de PMIP a una estación base y una pasarela o una pasarela y un anclaje de movilidad local (LMA).

[0043] Aunque se pueden ilustrar diversos ejemplos en el presente documento desde el punto de vista de una red UMB, las características descritas en el presente documento se pueden aplicar a otros tipos de redes, tal como WiMAX y LTE, por ejemplo.

[0044] La figura 1 es un diagrama de bloques de una red UMB en el que se pueden implementar una o más características de NAI seguro, perfil de usuario y distribución de políticas, y/o distribución de claves PMIP de acuerdo con un ejemplo. Una red UMB puede usar una arquitectura plana que no dependa de una entidad centralizada, tal como un controlador de estación base (BSC), para coordinar las conexiones a través de la estación

base evolucionada (eBS) de la UMB. Una eBS puede combinar las funciones de una estación base tradicional, un BSC y algunas funciones del nodo servidor de datos en paquetes (PDSN) en un único nodo, simplificando el despliegue de la red UMB. A medida que se reduce el número de componentes (en comparación con las redes de la técnica anterior), la red UMB puede ser más fiable, más flexible, más fácil de desplegar y/o menos costosa de hacer funcionar. Por ejemplo, en las redes heredadas, la BS, el BSC, el PDSN y el agente doméstico (HA) de IP móvil cooperan todos para dar servicio al tráfico de usuario. Las redes UMB reutilizan la mayor parte de la infraestructura de red central pero consolidan funciones en menos componentes de red. La combinación de estas funciones en menos nodos reduce la latencia, disminuye los costes de capital y mantenimiento, y reduce la complejidad de las interacciones entre los nodos para ofrecer QoS de extremo a extremo.

[0045] Este ejemplo ilustra cómo una red de acceso UMB 102 y una red servidora 113 pueden proporcionar acceso de red inalámbrica a una pluralidad de terminales de acceso AT 106, 108, 110, 122 (por ejemplo, pares de autenticación), en tanto que reutilizan una infraestructura de red central (por ejemplo, red doméstica 103). La red servidora 113 puede ser la red "doméstica" para los AT 106, 108, 110, 122, pero los AT también pueden recorrer o visitar otras redes y obtener conectividad de red inalámbrica desde dichas otras redes.

[0046] En este ejemplo, la red de acceso UMB 102 incluye una primera eBS 104 y una segunda eBS 107 (denominadas en líneas generales "nodos de acceso a red") que permiten que uno o más terminales de acceso (AT) 106, 108 y 110 se conecten con la red servidora 113 y la red doméstica 103. La primera eBS 104 se puede acoplar a un primer controlador de red de referencia de sesión (SRNC) 114 (denominado en líneas generales "autentificador") y una primera pasarela de acceso (AGW) 112 (denominada en líneas generales "nodo de pasarela de red") en la red servidora 113 que se acopla a la infraestructura de red doméstica 103. De manera similar, la segunda eBS 107 se puede acoplar a un segundo SRNC 109 y a la primera AGW 112. La red servidora 113 puede incluir la AGW-a 112 y la AGW-b 120 que están acopladas a la autenticación, autorización y contabilidad local (LAAA) 124 y una función de recursos y control de políticas de visita (vPCRF) 132 para facilitar las comunicaciones y/o la conectividad para las eBS y los AT. La red doméstica 103 puede incluir un agente doméstico (HA) 126, una AAA doméstica (HAAA) 128 y una PCRF doméstica (hPCRF) 130. Adicionalmente, otras redes de acceso 105 también se pueden acoplar al HA 126 y/o a la LAAA 124 para proporcionar conectividad de red inalámbrica para acceder a los terminales.

[0047] En diversas implementaciones, la red de acceso UMB 102 puede incluir otras eBS 116 y 117, SRNC 118, y AGW 120 que pueden proporcionar conectividad de red inalámbrica a otros AT 122. Las redes 102, 113, 105 y/o 103 están destinadas como un ejemplo de un sistema de comunicación en el que pueden funcionar una o más características novedosas descritas en el presente documento. Sin embargo, los dispositivos y/o la funcionalidad de esos dispositivos en estas redes se pueden localizar en las otras redes mostradas (o en una red diferente) sin apartarse del funcionamiento y las características descritas en el presente documento.

[0048] De acuerdo con diversos ejemplos, los AT 106, 108, 110 y/o 122 pueden ser dispositivos de comunicación inalámbricos, teléfonos móviles, terminales inalámbricos y otros tipos de dispositivos móviles y/o inalámbricos que admitan conectividad de radio inalámbrica a través de una red UMB.

[0049] Las eBS 104, 107 y 116 admiten la interfaz aérea UMB. Las eBS 104, 107 y/o 116 pueden incluir protocolos MAC y/o físicos UMB y pueden realizar gestión de recursos de radio, gestión de canales de radio, cifrado de capa 2 y/o compresión de cabecera IP (por ejemplo, ROHC).

[0050] La AGW 112 y/o 120 puede proporcionar conectividad IP de capa 3 a la red doméstica 103. La AGW 112 y/o 120 puede incluir diversas funciones tales como autenticación, almacenamiento en memoria intermedia de estado inactivo y/o cliente de IP móvil de proxy. Por ejemplo, la AGW 112 y/o 120 puede incluir gestión de dirección IP, agente externo (FA) para MIPv4, retransmisión DHCP, cliente de IP móvil de proxy (PMIP), clasificación/vigilancia de paquetes IP, autentificador EAP y/o cliente de AAA.

[0051] Los SRNC 114, 109 y 118 pueden controlar diversas funciones en apoyo de control de recursos de radio, incluyendo el almacenamiento de información de sesión, funciones de paginación y gestión de localización. Las funciones de SRNC pueden incluir, por ejemplo, (a) almacenamiento de información de sesión de interfaz aérea, (b) controlador de paginación, (c) gestión de localización y/o (d) autentificador de EAP para los AT. El primer SRNC 114 puede mantener información específica de acceso de radio para los AT 106 y 108, mientras que el segundo SRNC 107 puede mantener información específica de acceso de radio para el AT 110. Un SRNC puede ser responsable de mantener la referencia de sesión (por ejemplo, punto de almacenamiento de sesión para el contexto negociado de interfaz aérea), admitir la gestión de estado inactivo y proporcionar las funciones de control de paginación cuando el AT está inactivo. El SRNC también puede ser responsable de la autenticación de acceso del AT. La función SRNC puede estar alojada en, o ubicada con, una eBS o puede estar localizada en una entidad separada (sin radio). Téngase en cuenta que el SRNC se puede implementar tanto en una configuración centralizada como distribuida. En una configuración centralizada, un único SRNC 118 está conectado con varias eBS 116 y 117 y la AGW 120. En una configuración distribuida, cada eBS incluye un SRNC.

[0052] Los servicios de autenticación, autorización y contabilidad (AAA) para la red doméstica 103 se pueden dividir entre un agente doméstico 126, una AAA local (LAAA) 124 y una AAA doméstica (HAAA) 128. La HAAA 128 puede

ser responsable de la autenticación, autorización y contabilidad asociadas con el uso de los AT 106, 108, 110 y/o 112 de los recursos de red. Un agente local (HA) 126 puede proporcionar una solución de movilidad que admita, por ejemplo, IP móvil de cliente (CMIP) y/o IP móvil de proxy (PMIP) y también puede facilitar la movilidad entre tecnologías.

[0053] Una función de recursos y control de políticas (PCRF) puede almacenar y distribuir las políticas para los AT 106, 108, 110 y/o 122. En una implementación, una PCRF doméstica (hPCRF) 130 puede ser responsable de las políticas de la red doméstica y una PCRF visitante (vPCRF) 132 puede ser responsable de las políticas de red visitante. La hPCRF 130 y la vPCRF 132 proporcionan reglas locales y de visita, respectivamente, a las AGW 112 y 120. Estas reglas pueden incluir, por ejemplo, (a) detección de paquetes que pertenecen a un flujo de datos de servicio, (b) proporcionar control de políticas para un flujo de datos de servicio, y/o (c) proporcionar parámetros de facturación aplicables para un flujo de datos de servicio.

Asegurar el identificador de acceso a red anónimo

[0054] En virtud de las redes de la técnica anterior, tales como redes de datos en paquetes de alta velocidad (HRPD), los terminales de acceso AT envían sus identificadores de acceso a red (NAI) por vía aérea durante un proceso de autenticación. Dicha transmisión por vía aérea puede exponer el NAI a terceros y compromete la seguridad de las comunicaciones. Adicionalmente, el NAI se puede conocer por parte del PDSN para el informe de cuentas y la recuperación de políticas de la PCRF, por ejemplo.

[0055] La figura 2 es un diagrama de flujo que ilustra un procedimiento de autenticación mediante el cual un identificador de acceso a red (NAI) no se transmite por vía aérea durante una autenticación de acceso a red entre un terminal de acceso (AT) y la entidad de autenticación, autorización y contabilidad domésticas (HAAA). Por ejemplo, durante una suscripción inicial, tanto el AT 202 como la HAAA 216 pueden obtener un NAI asociado con el AT 202. Este NAI se puede almacenar en una tarjeta de módulo de identidad de abonado (SIM), por ejemplo, en el AT 202 y conocerse por la HAAA 216. En algunas implementaciones, también se puede obtener un pseudo-NAI durante el proceso de suscripción inicial. El pseudo-NAI se puede generar por la HAAA 216 o bien el AT 202 y conocerse tanto por la HAAA 216 como por el AT 202. El pseudo-NAI se puede asociar con el NAI para el AT 202, de modo que tanto la HAAA 216 como el AT 202 puedan usarlo durante un proceso de autenticación de acceso posterior.

[0056] Para establecer las comunicaciones con una eBS servidora 204, el AT 202 puede configurar una sesión de UMB 224. El AT puede entonces enviar una solicitud de autenticación de acceso 226a y 226b a la HAAA 216 a través de la eBS 204. La solicitud de autenticación de acceso 226 se puede enviar en un protocolo de autenticación extensible (EAP) (o algún otro protocolo de autenticación segura) por UMB a la eBS 204 y entonces en EAP por un protocolo AAA al HAAA 216. La solicitud de autenticación 226 puede incluir el pseudo-NAI (por ejemplo, obtenido durante la suscripción inicial) de modo que el AT 202 solicitante se pueda identificar por la HAAA 216 con fines de autenticación. En otras implementaciones, donde no se ha obtenido un pseudo-NAI desde la HAAA, el AT 202 puede enviar el NAI real en la solicitud de autenticación 226. Sin embargo, esto se hace solo la primera vez y se puede usar posteriormente un pseudo-NAI (por ejemplo, proporcionado por la HAAA 216), limitando de este modo la transmisión del NAI real por vía aérea

[0057] La HAAA 216 genera una ID de usuario que se puede asociar con el NAI o el AT 228 solicitante. Por ejemplo, la ID de usuario puede ser un número aleatorio generado por la HAAA, o puede ser una función de (al menos parcialmente) el NAI, o (en algunas implementaciones) puede ser el NAI.

[0058] La HAAA 216 también puede recuperar un perfil de usuario y perfil de usuario de QoS (por ejemplo, desde la hPCRF 214 o la vPCRF 208) en función del NAI para el AT 202 solicitante. En un ejemplo, el perfil de usuario y el perfil de usuario de QoS pueden definir el tipo de servicio, el plan de servicio, las restricciones de servicio, etc., asociados con el AT 202 solicitante. En algunas implementaciones, la HAAA 216 también puede generar un nuevo pseudo-NAI que puede enviar al AT 202 para que se use en solicitudes de autenticación posteriores.

[0059] Un mensaje de autenticación de acceso satisfactorio 232 se puede entonces enviar a la LAAA 210 que puede incluir la ID de usuario, el perfil de usuario, el perfil de usuario de QoS, y (posiblemente) el nuevo pseudo-NAI. A su vez, la LAAA 210 puede remitir la ID de usuario, el perfil de usuario y el perfil de usuario de QoS, y una clave MN-HA de PMIP al SRNC 204. El SRNC 204 puede proporcionar la clave MN-HA de PMIP a la AGW 206; posteriormente, el SRNC 204 y/o la AGW 206 puede usar esta ID de usuario para el informe contable y la recuperación de políticas sin conocimiento del NAI_1.

[0060] En el caso donde la ID de usuario es un número aleatorio (por ejemplo, asociado con el NAI por la HAAA), se puede usar la ID de usuario por la red servidora sin el conocimiento del NAI. Como resultado de este esquema, el NAI de los AT solicitantes no se envía por vía aérea y se conoce por un número limitado de entidades de infraestructura central (por ejemplo, la HAAA).

[0061] En otros casos, la ID de usuario puede ser el NAI pero se distribuye por la HAAA 216 a la red servidora y no se transmite por vía aérea por el AT 202.

[0062] La figura 3 ilustra un procedimiento de funcionamiento en un servidor de autenticación (por ejemplo, la HAAA) para una red de comunicación inalámbrica que se proporciona para asegurar una clave de usuario primario. Se recibe una solicitud de autenticación de acceso desde un par de autenticación inalámbrico (por ejemplo, el AT) 302. Se puede generar un identificador de usuario secundario (por ejemplo, la ID de usuario), en el que la clave de usuario secundario está asociada con un identificador de usuario primario (por ejemplo, el NAI) para el par de autenticación inalámbrico 304. La información de perfil de usuario (por ejemplo, el perfil de usuario) se puede recuperar en función del identificador de usuario primario 306. El identificador de usuario secundario se puede proporcionar a un autentificador (por ejemplo, el SNRC) asociado con el par de autenticación 308. La información del perfil de usuario se puede enviar al autentificador (por ejemplo, el SRNC). La red de comunicación puede incluir al menos una entre una red compatible de banda ancha ultra móvil (UMB), una red compatible con WiMAX o una red compatible de evolución a largo plazo (LTE). El servidor de autenticación (por ejemplo, HAAA) puede ser una entidad de autenticación, autorización y contabilidad (AAA), y el par de autenticación es un terminal de acceso (AT) inalámbrico. El autentificador puede ser un controlador de red de referencia de sesión (SRNC) asociado con una estación base (BS) que presta servicio al terminal de acceso inalámbrico (AT) en una red compatible de banda ancha ultra móvil (UMB) y el identificador de usuario primario es un identificador de acceso a red (NAI) para el terminal de acceso inalámbrico. La estación base servidora puede estar ubicada con el controlador de red de referencia de sesión (SRNC).

[0063] El identificador de usuario secundario puede ser un número generado aleatoriamente que posteriormente se asocia con el identificador de usuario primario. El identificador de usuario secundario también puede ser el identificador de usuario primario. El identificador de usuario secundario puede ser una función del identificador de usuario primario.

[0064] La figura 15 es un diagrama de bloques que ilustra un servidor de autenticación. El servidor de autenticación 1500 puede incluir un circuito de procesamiento 1504 acoplado a una interfaz de comunicación de red 1506. El circuito de procesamiento 1504 se puede adaptar para: (a) recibir una solicitud de autenticación de acceso desde un par de autenticación inalámbrico; (b) generar un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico; (c) proporcionar el identificador de usuario secundario a un autentificador asociado con el par de autenticación; (d) recuperar información de perfil de usuario en función del identificador de usuario primario; (e) proporcionar la información de perfil de usuario al autentificador.

[0065] En consecuencia, se puede proporcionar un servidor de autenticación que comprende: (a) un medio para recibir una solicitud de autenticación de acceso desde un par de autenticación inalámbrico; (b) un medio para generar un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico; (c) un medio para proporcionar el identificador de usuario secundario a un autentificador asociado con el par de autenticación; (d) un medio para recuperar información de perfil de usuario en función del identificador de usuario primario; y/o (e) un medio para proporcionar la información de perfil de usuario al autentificador.

[0066] También se puede proporcionar un programa de ordenador de funcionamiento en un servidor de autenticación para asegurar un identificador de usuario primario, que cuando se ejecuta por un procesador provoca que el procesador: (a) reciba una solicitud de autenticación de acceso desde un par de autenticación inalámbrico; (b) genere un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico; (c) proporcione el identificador de usuario secundario a un autentificador asociado con el par de autenticación; (d) recupere información de perfil de usuario en función del identificador de usuario primario; y/o (e) proporcione la información de perfil de usuario al autentificador.

Distribución de perfil de usuario y política para AGW

[0067] La figura 4 es un diagrama de bloques que ilustra cómo se puede proporcionar el servicio inalámbrico a un AT a medida que se desplaza desde una primera eBS a una segunda eBS en una red UMB. En redes UMB, se realizan más funciones cerca de la interfaz inalámbrica con el AT 406. Una de estas funciones es permitir que el AT 406 se desplace o recorra entre las eBS (por ejemplo, desde una primera eBS-A 408 en el tiempo t_0 a una segunda eBS-B 410 en un tiempo t_1) de la red de acceso 402 en tanto que hace dicha movilidad transparente para la red doméstica 404. Para mantener la movilidad del AT 406 oculta de la red doméstica 404, la AGW 412 en la red servidora 403 gestiona la remisión a la eBS que presta servicio actualmente.

[0068] Como se ilustra en la figura 2, el SRNC-A 412 puede ser parte del proceso de autenticación. La ruta del mensaje de solicitud de autenticación 226a y 226b (de la fig. 2) y el mensaje de autenticación satisfactorio 232 y 234 se ilustra en la figura 4. Si el AT 406 se autentica satisfactoriamente por la HAAA 416, el SRNC-A 412 recibe la ID de usuario, el perfil de usuario, el perfil de usuario de QoS, la clave MN-HA de PMIP. Sin embargo, cuando un AT se desplaza desde la primera eBS 408 a la segunda eBS 410 dentro de la misma red de acceso 402, la AGW 414 puede ocultar la movilidad de los AT a la infraestructura de red doméstica 404. Sin embargo, para conseguir esto, la AGW 414 debe conocer la información de perfil de usuario y de políticas para el AT 406 a fin de determinar

correctamente el tipo de servicio (por ejemplo, calidad de servicio, etc.) que se debe proporcionar a través de la segunda eBS-B 410.

[0069] Se proponen tres procedimientos alternativos para proporcionar la información de perfil de usuario a la AGW. En primer lugar, la AGW 414 puede recuperar el perfil de usuario a partir de la LAAA 418 y la política de usuario a partir de una PCRF cuando se establece un nuevo túnel de PMIP. Las figuras 5 y 6 ilustran cómo una AGW puede recuperar el perfil de usuario a partir de una LAAA cuando se establece un nuevo túnel de PMIP y la política de usuario a partir de una PCRF en configuraciones de SRNC distribuidas y centralizadas, respectivamente. En segundo lugar, la AGW 414 puede obtener la información del perfil de usuario durante un proceso de autenticación y la información de la política de usuario a partir de una PCRF. Las figuras 7 y 8 ilustran cómo una AGW puede obtener información de perfil de usuario como parte de un proceso de autenticación y de política de usuario a partir de una PCRF en configuraciones de SRNC distribuidas y centralizadas, respectivamente. En tercer lugar, la LAAA 418 puede impulsar el perfil de usuario a la AGW 414 y la AGW puede entonces solicitar la política de usuario a partir de la PCRF. Las figuras 9 y 10 ilustran cómo una LAAA puede impulsar el perfil de usuario a la AGW 414 y la AGW puede solicitar la política de usuario a partir de una PCRF en configuraciones de SRNC distribuidas y centralizadas, respectivamente.

[0070] Téngase en cuenta que en una configuración de SRNC distributiva, el SRNC puede ser ubicado con las eBS (por ejemplo, fig. 1 - eBS-a 114 y SRNC-a 104), en tanto que en una configuración de SRNC centralizada, el SRNC puede estar separado de la eBS y dar servicio a una o más eBS (por ejemplo, fig. 1 - SRNC-c 118, eBS-c 116 y eBS-d 117).

[0071] La figura 5 ilustra cómo una AGW puede recuperar el perfil de usuario a partir de una LAAA cuando se establece un nuevo túnel de PMIP y solicitar la política de usuario desde la PCRF en una configuración de SRNC distribuida. Se puede realizar un proceso de autenticación 520, 522, 524 y 525 donde el AT 502 envía una solicitud de autenticación a la HAAA 516. Si el AT se autentica por la HAAA 616, la HAAA 616 genera una ID de usuario y otra información de perfil de usuario en respuesta. Como parte de la respuesta de autenticación 525, la eBS/SRNC 504 puede recibir el perfil de usuario desde la LAAA 510.

[0072] Una vez que la autenticación de acceso se ha realizado, el AT 502 se puede desplazar desde una eBS 504 de punto de anclaje de datos (DAP) a una nueva eBS servidora. La nueva eBS servidora puede enviar una solicitud de desplazamiento de DAP 530 a través de la nueva eBS servidora/SRNC. Un mensaje de solicitud de registro (RRQ) de IP móvil de proxy (PMIP) 532 (que incluye una ID de usuario para el AT 502) se envía por la nueva eBS servidora/SRNC a la AGW 506 que, a su vez, envía un mensaje de solicitud de AAA (ID de usuario) 534 a la LAAA 510. La LAAA 510 recupera la información de perfil de usuario (por ejemplo, perfil de usuario, clave MN-HA de PMIP, etc.) asociada con el AT solicitante y la envía a la AGW 506. La AGW 506 puede enviar un mensaje de respuesta de registro (RRP) de PMIP 538 a la eBS/SRNC 504 que entonces envía un mensaje de asignación de desplazamiento de DAP 540 al AT 502.

[0073] Durante un proceso en el que se puede asociar una nueva dirección IP y/o configuración 542 con el AT 502, la AGW 506 (con el conocimiento de la ID de usuario), puede obtener la política de usuario para el AT asociado con la ID de usuario. La AGW 506 puede enviar una solicitud de política (ID de usuario) 544 a la vPCRF 508 que se puede remitir 546 a la hPCRF 514. Debido a que la hPCRF 514 no conoce la asignación entre la ID de usuario y el NAI asociados con la política de usuario, puede entonces enviar una solicitud de NAI (ID de usuario) 548 a la HAAA 516. La HAAA 516 responde con una respuesta de NAI (ID de usuario, NAI) 550 que la hPCRF 514 puede usar para obtener la política de usuario asociada con la ID de usuario y el NAI. Es decir, la hPCRF 514 usa el NAI para obtener la política de usuario correspondiente al AT asociado con la ID de usuario. Una respuesta de políticas (ID de usuario, política de usuario) 552 se envía por parte de la hPCRF 514 a la vPCRF 508 que entonces envía una respuesta de políticas (ID de usuario, política de usuario) 554 a la AGW 506. La AGW 506 puede entonces impulsar o enviar 556 la política de usuario a la eBS/SRNC 504.

[0074] De acuerdo con un ejemplo, el AT 502 puede autorizar la recuperación de la información del perfil de usuario y/o de las políticas incluyendo un MAC en el mensaje de solicitud de desplazamiento de DAP 530. El MAC se puede crear en función de ciertos datos estáticos, junto con cierta información dinámica, tal como un número de secuencia. La clave para la generación de MAC se puede derivar de una jerarquía de claves de EAP (por ejemplo, una clave de la DSRK, clave raíz específica de dominio) compartida entre el AT 502 y la HAAA 516 (o la LAAA). Por ejemplo, la clave de generación de MAC se puede basar en una clave de autorización, AK, que es parte de la jerarquía de claves de EAP (por ejemplo, AK = f(DSRK), donde f es cierta función, tal como una función pseudoaleatoria como HMAC_SHA256). Los datos de autorización incluidos en el mensaje de solicitud de desplazamiento de DAP 530 del AT 502 se pueden enviar a la LAAA 510 a través de la AGW 506. Tras la verificación satisfactoria del MAC, la LAAA 510 envía el perfil de usuario a la AGW 506.

[0075] Para la recuperación de políticas a partir de la PCRF, se podría usar un enfoque similar. La clave usada en este caso debe provenir de la clave compartida entre el AT y la HAAA (se puede generar una clave desde el EMSK de EAP de manera similar a la anterior).

[0076] La figura 6 ilustra cómo una AGW puede recuperar el perfil de usuario desde una LAAA cuando se establece un nuevo túnel de PMIP y solicitar la política de usuario a partir de la PCRF en una configuración de SRNC centralizada. Se puede realizar un proceso de autenticación 622, 624, 626 y 625 donde el AT 602 envía una solicitud de autenticación a la HAAA 618. Si el AT 602 se autentica satisfactoriamente por parte de la HAAA 618, la HAAA 618 genera una ID de usuario y obtiene otra información de perfil de usuario en respuesta. Como parte de la respuesta de autenticación, el SRNC 606 puede recibir 625 el perfil de usuario desde la LAAA 610.

[0077] Una vez que la autenticación de acceso se ha realizado, el AT 602 se puede desplazar desde una eBS 604 de punto de anclaje de datos (DAP) a una nueva eBS servidora. Un mensaje de RRQ de IP móvil de proxy (PMIP) 632 (que incluye una ID de usuario para el AT 602) se envía por parte de la nueva eBS servidora a la AGW 608 que, a su vez, envía un mensaje de solicitud de AAA 634 (incluyendo la ID de usuario para el AT 602) a la LAAA 612. La LAAA 612 recupera la información de perfil de usuario (por ejemplo, el perfil de usuario, la clave MN-HA de PMIP, etc.) asociada con el AT solicitante 602 y la envía a la AGW 608. La AGW 608 puede enviar un mensaje de RRP de PMIP 637 a la nueva eBS servidora que entonces envía un mensaje de asignación de desplazamiento de DAP 639 al AT 602.

[0078] Para las implementaciones ilustradas en las figuras 5 y 6, si la seguridad es la preocupación, se puede incluir la firma del AT (por ejemplo, un código de comprobación de la clave MN-HA) en la solicitud de desplazamiento de DAP/RRQ de PMIP y la HAAA puede verificarlo antes de enviar el NAI (asociado con el AT solicitante) a la hPCRF para recuperar la información del perfil de usuario y/o de las políticas.

[0079] Durante un proceso en el que se puede asociar una nueva dirección IP y/o configuración 638 con el AT 602, la AGW 608 (con el conocimiento de la ID de usuario) puede ser capaz de obtener la política de usuario para el AT asociado con la ID de usuario. La AGW 608 puede entonces enviar una solicitud de políticas (ID de usuario) 640 a la vPCRF 610 que se puede remitir 642 a la hPCRF 616. Debido a que la hPCRF 616 no conoce la asignación entre la ID de usuario y el NAI asociados con la política de usuario, puede entonces enviar una solicitud de NAI (ID de usuario) 644 a la HAAA 618. La HAAA 618 responde con una respuesta de NAI (ID de usuario, NAI) 646 que la hPCRF 616 puede usar para obtener la política de usuario asociada con la ID de usuario y el NAI. Es decir, la hPCRF 616 usa el NAI para obtener la política de usuario correspondiente al AT asociado con la ID de usuario. Una respuesta de políticas (ID de usuario, política de usuario) 648 se envía por parte de la hPCRF 616 a la vPCRF 610 que entonces envía una respuesta de políticas (ID de usuario, política de usuario) 650 a la AGW 608. La AGW 608 puede entonces impulsar o enviar la política de usuario al SRNC 606 que puede copiar parte o la totalidad de dicha información 654 a la eBS 604.

[0080] La figura 7 ilustra cómo una AGW puede obtener información de perfil de usuario como parte de un proceso de autenticación y de política de usuario a partir de una PCRF en una configuración de SRNC distribuida. Se puede realizar un proceso de autenticación 720, 722, 724, 728 donde el AT 702 envía una solicitud de autenticación a la HAAA 716. Si el AT 702 se autentica satisfactoriamente por parte de la HAAA 716, la HAAA 716 genera una ID de usuario y obtiene otra información de perfil de usuario en respuesta. Como parte de la respuesta de autenticación, el SRNC 706 puede recibir el perfil de usuario desde la LAAA 710. La eBS/SRNC 704 puede entonces recibir información de perfil de usuario (por ejemplo, la ID de usuario, el perfil de usuario y/o la clave MN-HA de PMIP) desde la AGW 706.

[0081] Durante un proceso en el que una nueva dirección IP y/o configuración 738 pueden estar asociadas con el AT 702, la AGW 706 (con el conocimiento de la ID de usuario) puede ser capaz de obtener la política de usuario para el AT asociado con la ID de usuario. La AGW 706 puede enviar una solicitud de políticas (ID de usuario) 740 a la vPCRF 708 que se puede remitir 742 a la hPCRF 714. Debido a que la hPCRF 714 no conoce la asignación entre la ID de usuario y el NAI asociados con la política de usuario, puede entonces enviar una solicitud de NAI (ID de usuario) 744 a la HAAA 716. La HAAA 716 responde con una respuesta de NAI (ID de usuario, NAI) 746 que la hPCRF 714 puede usar para obtener la política de usuario asociada con la ID de usuario y el NAI. Es decir, la hPCRF 714 usa el NAI para obtener la política de usuario correspondiente al AT asociado con la ID de usuario. Una respuesta de políticas (ID de usuario, política de usuario) 748 se envía por parte de la hPCRF 714 a la vPCRF 708 que entonces envía una respuesta de políticas (ID de usuario, política de usuario) 748 a la AGW 706. La AGW 706 puede entonces impulsar o enviar la política de usuario a la eBS/SRNC 704.

[0082] La figura 8 ilustra cómo una AGW puede obtener información de perfil de usuario como parte de un proceso de autenticación y de política de usuario a partir de una PCRF en una configuración de SRNC distribuida. Como parte de una autenticación de acceso, el SRNC 806 puede recibir información de perfil de usuario (por ejemplo, la ID de usuario, el perfil de usuario y/o la clave MN-HA de PMIP). El SRNC 806 puede entonces impulsar o enviar la información de perfil de usuario (por ejemplo, la ID de usuario, el perfil de usuario y/o la clave MN-HA de PMIP) a la AGW 808 en un mensaje de solicitud de AAA 828 y recibe un mensaje de acuse de recibo de AAA 830 desde la AGW 808.

[0083] Se puede realizar un proceso de autenticación 822, 824, 826, 828 donde el AT 802 envía una solicitud de autenticación a la HAAA 818. Si el AT 802 se autentica satisfactoriamente por parte de la HAAA 818, la HAAA 818 genera una ID de usuario y obtiene otra información de perfil de usuario en respuesta. Como parte de la respuesta

de autenticación, la AGW 808 puede recibir la información de perfil de usuario (por ejemplo, la ID de usuario, el perfil de usuario y/o la clave MN-HA de PMIP) desde la LAAA 812. La AGW 808 puede entonces remitir esta información de perfil de usuario al SRNC 806, que puede copiar 832 parte o la totalidad de esta a la eBS 804.

[0084] Una vez que la autenticación de acceso se ha realizado, el AT 802 se puede desplazar desde una eBS 804 de punto de anclaje de datos (DAP) a una nueva eBS servidora. Durante un proceso en el que se puede asociar una nueva dirección IP y/o configuración 842 con el AT 802, la AGW 808 (con conocimiento de la ID de usuario) puede ser capaz de obtener la política de usuario para el AT asociado con la ID de usuario. La AGW 808 puede enviar una solicitud de políticas (ID de usuario) 844 a la vPCRF 810 que se puede remitir 846 a la hPCRF 816. Debido a que la hPCRF 816 no conoce la asignación entre la ID de usuario y el NAI asociados con la política de usuario, puede entonces enviar una solicitud de NAI (ID de usuario) 848 a la HAAA 818. La HAAA 818 responde con una respuesta de NAI (ID de usuario, NAI) 850 que la hPCRF 816 puede usar para obtener la política de usuario asociada con la ID de usuario y el NAI. Es decir, la hPCRF 816 usa el NAI para obtener la política de usuario correspondiente al AT asociado con la ID de usuario. Una respuesta de políticas (ID de usuario, política de usuario) 852 se envía por parte de la hPCRF 816 a la vPCRF 810 que entonces envía una respuesta de políticas (ID de usuario, política de usuario) 854 a la AGW 808. La AGW 808 puede entonces impulsar o enviar 856 la política de usuario al SRNC 806, que puede copiar 858 parte o la totalidad de dicha información a la eBS 804.

[0085] La figura 9 ilustra cómo una LAAA puede impulsar el perfil de usuario a la AGW 414 y la AGW puede solicitar la política de usuario desde una PCRF en una configuración de SRNC distribuida. Se puede realizar un proceso de autenticación 920, 922 y 924 donde el AT 902 envía una solicitud de autenticación a la HAAA 916. Si el AT se autentica por la HAAA 916, la HAAA 916 genera una ID de usuario y otra información de perfil de usuario en respuesta. Como parte de la respuesta de autenticación, la eBS/SRNC 904 puede recibir el perfil de usuario desde la LAAA 910. Posteriormente, la LAAA 910 puede impulsar o enviar un mensaje de AAA (ID de usuario, perfil de usuario, clave MN-HA de PMIP) 926 a la AGW 906. La AGW 906 puede acusar 928 recibo del mensaje 926. Se puede obtener la política de usuario por la AGW mediante un proceso similar a los procesos ilustrados en las figuras 5 y 7.

[0086] La figura 10 ilustra cómo una LAAA puede impulsar el perfil de usuario a una AGW y la AGW puede solicitar la política de usuario desde una PCRF en una configuración de SRNC centralizada. Se puede realizar un proceso de autenticación 1022, 1024 y 1026 donde el AT 1002 envía una solicitud de autenticación a la HAAA 1018. Si el AT 1002 se autentica por parte de la HAAA 1018, la HAAA 1018 genera una ID de usuario y otra información de perfil de usuario en respuesta. Como parte de la respuesta de autenticación, el SRNC 1006 puede recibir el perfil de usuario desde la LAAA 1012. Posteriormente, la LAAA 1012 puede impulsar o enviar un mensaje de AAA (ID de usuario, perfil de usuario, clave MN-HA de PMIP) 1028 a la AGW 1008. La AGW 1008 puede acusar 1030 recibo del mensaje 1028. La política de usuario se puede obtener por la AGW mediante un proceso similar al proceso ilustrado en las figuras 5 y 7 y 9.

[0087] La figura 11 ilustra un procedimiento de funcionamiento de un servidor de autenticación para proporcionar un autentificador con información de perfil de usuario. Un servidor de autenticación (por ejemplo, una HAAA) puede recibir una solicitud de autenticación de acceso desde el par de autenticación (por ejemplo, el AT) 1100 y verifica si el par de autenticación es un abonado válido de la red de comunicación (por ejemplo, una red UMB). Un servidor de autenticación puede autenticar a un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red 1102. Si el par de autenticación se autentica satisfactoriamente por parte del servidor de autenticación 1104, el servidor de autenticación recupera la información de perfil de usuario asociada con el par de autenticación 1106. El servidor de autenticación envía entonces la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación 1108. De manera similar, el servidor de autenticación también puede enviar la información de perfil de usuario a un autentificador que facilita las comunicaciones para el par de autenticación 1110. Dicha información de perfil de usuario puede proporcionar, por ejemplo, un grado o calidad de servicio para el par de autenticación. En un ejemplo, el servidor de autenticación puede ser una entidad de autenticación, autorización y contabilidad (AAA) que es parte de la red de comunicación. En una implementación, el envío de la información de perfil de usuario al nodo de pasarela de red puede incluir hacer que el autentificador envíe la información de perfil de usuario al nodo de pasarela de red. La información de perfil de usuario se puede proporcionar de acuerdo con uno o más de los procedimientos ilustrados en las figuras 5-10.

[0088] Con referencia de nuevo a la figura 15, el circuito de procesamiento 1504 del servidor de autenticación 1500 se puede adaptar para: (a) autenticar un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red; (b) recuperar la información de perfil de usuario asociada con el par de autenticación; (c) enviar la información de perfil de usuario a un nodo de pasarela de red que facilite los servicios de comunicación para el par de autenticación; (d) enviar la información de perfil de usuario a un autentificador que facilite las comunicaciones para el par de autenticación; (e) recibir una solicitud de identificador de usuario primario desde una entidad PCRF, en la que el identificador de usuario primario esté asociado exclusivamente con el par de autenticación; y/o (f) enviar una respuesta a la entidad PCRF que incluya el identificador de usuario primario solicitado.

[0089] En consecuencia, se puede proporcionar un servidor de autenticación que comprende: (a) un medio para autenticar un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red; (b) un medio para recuperar información de perfil de usuario asociada con el par de autenticación; (c) un medio para enviar la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación; (d) un medio para enviar la información de perfil de usuario a un autentificador que facilite las comunicaciones para el par de autenticación; (e) un medio para recibir una solicitud de identificador de usuario primario desde una entidad PCRF, en el que el identificador de usuario primario está asociado exclusivamente con el par de autenticación; y/o (f) un medio para enviar una respuesta a la entidad PCRF que incluya el identificador de usuario primario solicitado.

[0090] De manera similar, también se puede proporcionar un programa informático de funcionamiento en un servidor de autenticación para proporcionar información de usuario, que cuando se ejecuta por un procesador provoca que el procesador: (a) autentique un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red; (b) recupere información de perfil de usuario asociada con el par de autenticación; (c) envíe la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación; (d) envíe la información de perfil de usuario a un autentificador que facilita las comunicaciones para el par de autenticación; (e) reciba una solicitud de identificador de usuario primario desde una entidad PCRF, en la que el identificador de usuario primario está asociado exclusivamente con el par de autenticación; y/o (f) envíe una respuesta a la entidad PCRF que incluya el identificador de usuario primario solicitado.

[0091] La figura 12 ilustra un procedimiento para proporcionar un nodo de pasarela de red con información de política de usuario para un par de autenticación de funcionamiento en una red de comunicación. El procedimiento puede comprender: (a) enviar una solicitud de políticas desde el nodo de pasarela de red a una entidad de función de recursos y control de políticas (PCRF) 1202, en la que la solicitud de políticas puede ser para una política de usuario para un par de autenticación al que el nodo de pasarela de red facilita las comunicaciones; (b) enviar una solicitud de identificador de usuario primario desde la entidad PCRF al servidor de autenticación, en la que el identificador de usuario primario está asociado exclusivamente con el par de autenticación 1204; (c) enviar una respuesta desde el servidor de autenticación a la entidad PCRF que incluye el identificador de usuario primario solicitado 1206; (d) obtener una política de usuario en la entidad PCRF para el par de autenticación que usa el identificador de usuario primario 1208; y/o (e) enviar la política de usuario desde la entidad PCRF al nodo de pasarela de red 1210. Por ejemplo, la información de política de usuario se puede proporcionar de acuerdo con uno o más de los procedimientos ilustrados en las figuras 5-10. El autentificador puede ser un controlador de red de referencia de sesión (SRNC) asociado con una estación base que presta servicio al par de autenticación en una red compatible de banda ancha ultra móvil (UMB), y el identificador confidencial es un identificador de acceso a red para el terminal de acceso inalámbrico.

Distribución de clave de PMIP para verificar nuevas solicitudes de túnel

[0092] A medida que un AT recorre o se desplaza a diferentes eBS, la AGW que gestiona las comunicaciones para el AT establece un túnel de IP móvil de proxy (PMIP) a las nuevas eBS servidoras. Sin embargo, la AGW tiene que prevenir que otras eBS (o intrusos) afirmen que van a proporcionar conectividad inalámbrica al AT cuando no lo van a hacer. La AGW debería poder prevenir que una entidad no autorizada cambie la conexión de túnel de PMIP. De este modo, se puede usar una clave de agente doméstico de nodo móvil (MN-HA) para asegurar los túneles de PMIP entre la eBS y la AGW y entre el SRNC y la AGW.

[0093] Existen al menos dos tipos de túneles de PMIP, túneles de PMIP RAN entre una eBS y una AGW y túneles de PMIP de red entre una AGW y un SRNC y entre una primera AGW y una segunda AGW. A medida que un AT se desplaza desde eBS a eBS (dentro de una red servidora), se puede establecer un nuevo túnel de PMIP RAN por la AGW con la nueva eBS servidora. De manera similar, a medida que el AT se desplaza o recorre una nueva red de acceso o servicio, la AGW doméstica puede establecer un túnel de PMIP de red con la nueva red de acceso o servidora.

[0094] Existen varias maneras de obtener una clave de MN-HA que se puede usar para verificar si se debe establecer un nuevo túnel de PMIP por una AGW. La LAAA simplemente puede elegir un número aleatorio ya que la clave de MN-HA del túnel de PMIP lo proporciona a la AGW. Ya que el AT no necesita conocer esta clave, la única entidad que "deriva" esta clave es la LAAA. De ahí que no haya necesidad de una derivación ya que una simple generación segura de números aleatorios es suficiente. El número aleatorio generado (es decir, la clave de MN-HA) se puede suministrar al SRNC y/o a la AGW para su uso en la verificación de si se debe establecer un nuevo túnel de PMIP (por ejemplo, un túnel de PMIPv4).

[0095] De forma alternativa, se puede crear una clave de MN-HA a partir de la jerarquía de EAP, como en el caso de la clave de autenticación. Por ejemplo, la clave de MN-HA puede ser una función de la DSRK (clave raíz específica de dominio) compartida entre el AT y la LAAA (por ejemplo, DSRK -> P4K (clave de MN-HA de PMIPv4) o P4K = f(DSRK), donde f es cierta función (por ejemplo, función pseudoaleatoria, tal como HMAC_SHA256). El P4K generado (es decir, la clave de MN-HA) se puede suministrar al SRNC y/o a la AGW para que se pueda asegurar un túnel de PMIP (por ejemplo, un túnel de PMIPv4).

[0096] En ciertas implementaciones, se puede enviar una clave de MN-HA a la AGW junto con el perfil de usuario. Por ejemplo, se puede enviar la clave de MN-HA a un SRNC servidor a través de una autenticación de acceso satisfactoria. En todavía otras implementaciones, se puede generar la clave de MN-HA por la propia AGW y distribuirse a la eBS servidora actual.

[0097] Cuando un móvil en primer lugar establece las comunicaciones en una red servidora a través de una eBS, esa eBS y su AGW están provistas de una clave de MN-HA (que se puede obtener como se analizó anteriormente. Cuando la AGW recibe una solicitud de desplazamiento de DAP, puede verificar si la eBS solicitante conoce la clave de MN-HA. Si la conoce, la AGW puede aceptar la solicitud de desplazamiento. Sin embargo, si la eBS solicitante no conoce la clave de MN-HA, la AGW puede denegar la solicitud de desplazamiento ya que no se puede confiar en la eBS solicitante. De manera similar, se puede usar la clave de MN-HA para proteger solicitudes de desplazamiento desde diferentes AGW o HA.

[0098] Con referencia de nuevo a la figura 1, en un ejemplo un terminal de acceso AT-x 122 puede establecer el servicio inalámbrico a través de la eBS-c 116. Durante el proceso de establecer su servicio inalámbrico, el AT-x 122 se puede autenticar a sí mismo con las redes servidoras y domésticas (por ejemplo, como se analiza e ilustra con referencia a las fig. 5-10). En un ejemplo (donde se usa un SRNC centralizado), como parte de este proceso de autenticación, se puede proporcionar a (o generar por) la AGW-c 120 una clave de MN-HA. La clave de MN-HA también se proporciona al SRNC-c servidor 118 que admite la eBS-c servidora 116. Si en un tiempo posterior el AT-x 122 se desplaza a la eBS-d 117, se puede generar una solicitud de desplazamiento de DAP mediante la cual se debe establecer un nuevo túnel de PMIP entre la nueva eBS-d 117 y la AGW-c servidora 120. Ya que el SRNC-c 118 conoce la clave de MN-HA (del proceso de autenticación previo), puede proporcionar la clave de MN-HA a la AGW-c 120 para verificar que la nueva solicitud de túnel sea válida. En consecuencia, la AGW-c 120 puede establecer el nuevo túnel con la eBS-d 117 según lo solicitado.

[0099] En otro ejemplo, el AT-1 106 inicialmente realiza un proceso de autenticación a medida que busca servicio inalámbrico a través de la eBS-a 104. En consecuencia, la AGW-a 112 y el SRNC-a 114 conocerán la clave de MN-HA para su túnel. Si el AT-1 106 posteriormente se desea comunicar a través de la eBS-b 107, se envía una nueva solicitud de túnel a la AGW-a 112. Sin embargo, en este caso, el nuevo SRNC-b servidor 109 no conoce la clave de MN-HA (por ejemplo, se suministró inicialmente a SRNC-a 114). De este modo, a fin de verificar que su nueva solicitud de túnel sea válida, el SRNC-b 109 puede obtener la clave de MN-HA a partir del SRNC-a 114. Esto permite a la AGW reencaminar los datos a la nueva eBS-b servidora 107 sin la necesidad de una nueva autenticación. De forma alternativa, el AT-1 106 simplemente puede volver a autenticarse (por ejemplo, realizar el proceso de autenticación ilustrado en las fig. 5-10) con la red servidora y/o doméstica.

[0100] La figura 13 ilustra un procedimiento para verificar nuevas solicitudes de túnel en una red de comunicación. La conectividad de red inalámbrica se puede proporcionar a un par de autenticación a través de un primer nodo de acceso a red 1302. Se proporciona una clave de IP móvil de proxy (PMIP) a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y un nodo de red de PMIP usado para proporcionar comunicaciones al par de autenticación 1304. La clave de PMIP se proporciona entonces a un primer autentificador asociado al primer nodo de acceso a red 1306 (por ejemplo, a través del túnel de PMIP). Las comunicaciones se pueden entonces encaminar al primer nodo de acceso a red 1308.

[0101] Posteriormente, se puede recibir una solicitud en el nodo de red de PMIP desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación 1310. El nodo de red de PMIP puede verificar si la entidad solicitante conoce la clave de PMIP 1312. En un ejemplo, se pueden reencaminar las comunicaciones a un segundo nodo de acceso a red (por ejemplo, una nueva eBS) si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. En otro ejemplo, se pueden reencaminar las comunicaciones a un segundo nodo de pasarela de red (por ejemplo, la AGW) si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. El reencaminamiento de las comunicaciones puede incluir el establecimiento de un nuevo túnel de IP móvil de proxy entre el primer nodo de red de PMIP y una nueva entidad de red servidora 1314. En un ejemplo, se puede generar la clave de PMIP en una entidad de autenticación, autorización y contabilidad (AAA) o un nodo de pasarela de red. El nodo de red de PMIP puede ser un nodo de pasarela de red.

[0102] La figura 16 es un diagrama de bloques que ilustra un ejemplo de un dispositivo de nodo de red de PMIP. El dispositivo de nodo de red de PMIP 1600 puede incluir un circuito de procesamiento 1604 acoplado a una interfaz de comunicación de red 1606. El circuito de procesamiento 1604 se puede adaptar para: (a) proporcionar conectividad de red inalámbrica a un par de autenticación a través de un primer nodo de acceso a red; (b) proporcionar una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y el nodo de red de PMIP usado para proporcionar comunicaciones al par de autenticación; (c) proporcionar la clave de PMIP a un primer autentificador asociado al primer nodo de acceso a red; (d) recibir una solicitud desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación; (e) verificar si la entidad solicitante conoce la clave de PMIP; (f) reencaminar las comunicaciones a un segundo nodo de acceso a red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP; y/o (g) reencaminar las comunicaciones a un segundo nodo de pasarela de red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. El

reencaminamiento de las comunicaciones puede incluir el establecimiento de un nuevo túnel de IP móvil de proxy entre el primer nodo de red de PMIP y una nueva entidad de red servidora.

[0103] En consecuencia, también se puede proporcionar un dispositivo de nodo de red de PMIP, que comprende: (a) un medio para proporcionar conectividad de red inalámbrica a un par de autenticación a través de un primer nodo de acceso a red; (b) un medio para proporcionar una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y el nodo de red de PMIP usado para proporcionar comunicaciones al par de autenticación; (c) un medio para proporcionar la clave de PMIP a un primer autentificador asociado al primer nodo de acceso a red; recibir una solicitud desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación; (d) un medio para verificar si una entidad solicitante conoce la clave de PMIP; (e) un medio para reencaminar las comunicaciones a un segundo nodo de acceso a red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP; y/o (f) un medio para reencaminar las comunicaciones a un segundo nodo de pasarela de red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP. El reencaminamiento de las comunicaciones puede incluir el establecimiento de un nuevo túnel de IP móvil de proxy entre el primer nodo de red de PMIP y una nueva entidad de red servidora.

[0104] De manera similar, también se pueden proporcionar un programa informático de funcionamiento en un dispositivo de nodo de red de PMIP, que cuando se ejecuta por un procesador provoca que el procesador: (a) proporcione conectividad de red inalámbrica a un par de autenticación a través de un primer nodo de acceso a red; (b) proporcione una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y el nodo de red de PMIP usado para proporcionar las comunicaciones al par de autenticación; (c) proporcione la clave de PMIP a un primer autentificador asociado al primer nodo de acceso a red; (d) reciba una solicitud desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación; (e) verifique si la entidad solicitante conoce la clave de PMIP; (f) reencamine las comunicaciones a un segundo nodo de acceso a red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP; y/o (g) reencamine las comunicaciones a un segundo nodo de pasarela de red si la entidad solicitante demuestra satisfactoriamente que conoce la clave de PMIP.

[0105] Uno o más de los componentes, etapas y/o funciones ilustrados en las figuras 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15 y/o 16 se pueden disponer de nuevo y/o combinarse en un único componente, etapa o función o incluirse en varios componentes, etapas o funciones. También se pueden agregar elementos, componentes, etapas y/o funciones adicionales. El aparato, dispositivos y/o componentes ilustrados en las figuras 1, 4, 14, 15 y 16 se pueden configurar o adaptar para realizar uno o más de los procedimientos, características o etapas descritos en las figuras 2, 3 y/o 5-13. Los algoritmos descritos en el presente documento se pueden implementar eficientemente en software y/o integrarse en hardware.

[0106] Los expertos en la técnica apreciarán, además, que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos descritos en relación con las configuraciones divulgadas en el presente documento se pueden implementar como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito diversos componentes, bloques, módulos, circuitos y etapas ilustrativos, en general, en lo que respecta a su funcionalidad. Si dicha funcionalidad se implementa como hardware o software depende de la aplicación particular y de las restricciones de diseño impuestas al sistema global.

[0107] Cabe destacar que las configuraciones anteriores son simplemente ejemplos y no se deben interpretar como limitantes de las reivindicaciones. La descripción de las configuraciones pretende ser ilustrativa, y no limitar el alcance de las reivindicaciones. Como tal, las presentes enseñanzas se pueden aplicar fácilmente a otros tipos de aparatos y muchas alternativas, modificaciones y variaciones serán evidentes para los expertos en la técnica.

REIVINDICACIONES

1. Un procedimiento de funcionamiento en un servidor de autenticación para una red de comunicación inalámbrica, que comprende:

recibir una solicitud de autenticación de acceso desde un par de autenticación inalámbrico;

generar un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico, en el que el identificador de usuario primario es un identificador de acceso a pseudo-red obtenido durante un proceso de suscripción inicial;

proporcionar el identificador de usuario secundario a un autentificador asociado con el par de autenticación.

2. El procedimiento de la reivindicación 1, en el que la red de comunicación incluye al menos una entre una red compatible con banda ancha ultra móvil, UMB, una red compatible con WiMAX o una red compatible con evolución a largo plazo, LTE.

3. El procedimiento de la reivindicación 1, en el que el servidor de autenticación es una entidad de autenticación, autorización y contabilidad, AAA, y el par de autenticación es un terminal de acceso inalámbrico, AT.

4. El procedimiento de la reivindicación 3, en el que el autentificador es un controlador de red de referencia de sesión, SNRC, asociado a una estación base, BS, que presta servicio el terminal de acceso inalámbrico, AT, en una red compatible con banda ancha ultra móvil, UMB y el identificador de usuario primario es un identificador de acceso a red, NAI, para el terminal de acceso inalámbrico.

5. El procedimiento de la reivindicación 4, en el que la estación base servidora está ubicada con el controlador de red de referencia de sesión, SNRC.

6. El procedimiento de la reivindicación 1, que comprende además:

recuperar información de perfil de usuario en función del identificador de usuario primario; y

proporcionar la información de perfil de usuario al autentificador.

7. El procedimiento de la reivindicación 1, en el que el identificador de usuario secundario es un número generado aleatoriamente que se asocia posteriormente con el identificador de usuario primario.

8. El procedimiento de la reivindicación 1, en el que el identificador de usuario secundario es el identificador de usuario primario, o
una función del identificador de usuario primario.

9. Un servidor de autenticación que comprende:

un medio para recibir una solicitud de autenticación de acceso desde un par de autenticación inalámbrico;

un medio para generar un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico, en el que el identificador de usuario primario es un identificador de acceso a pseudo-red obtenido durante un proceso de suscripción inicial; y

un medio para proporcionar el identificador de usuario secundario a un autentificador asociado con el par de autenticación.

10. Un procedimiento de funcionamiento en una red de comunicación, que comprende:

autenticar a un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red;

recuperar información de perfil de usuario asociada con el par de autenticación, en la que la información de perfil de usuario se basa en un identificador de usuario primario que es un identificador de acceso a pseudo-red obtenido durante un proceso de suscripción inicial; y

enviar la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación.

11. Un servidor de autenticación que comprende:

un medio para autenticar un par de autenticación que busca establecer comunicaciones a través de un primer nodo de acceso a red;

un medio para recuperar información de perfil de usuario asociada con el par de autenticación, en el que la información de perfil de usuario se basa en un identificador de usuario primario que es un identificador de acceso a pseudo-red obtenido durante un proceso de suscripción inicial; y

un medio para enviar la información de perfil de usuario a un nodo de pasarela de red que facilita los servicios de comunicación para el par de autenticación.

12. Un programa informático de funcionamiento en un servidor de autenticación que, cuando se ejecuta por un procesador, provoca que el procesador lleve a cabo las etapas de cualquiera de las reivindicaciones 1 a 8 o 10.

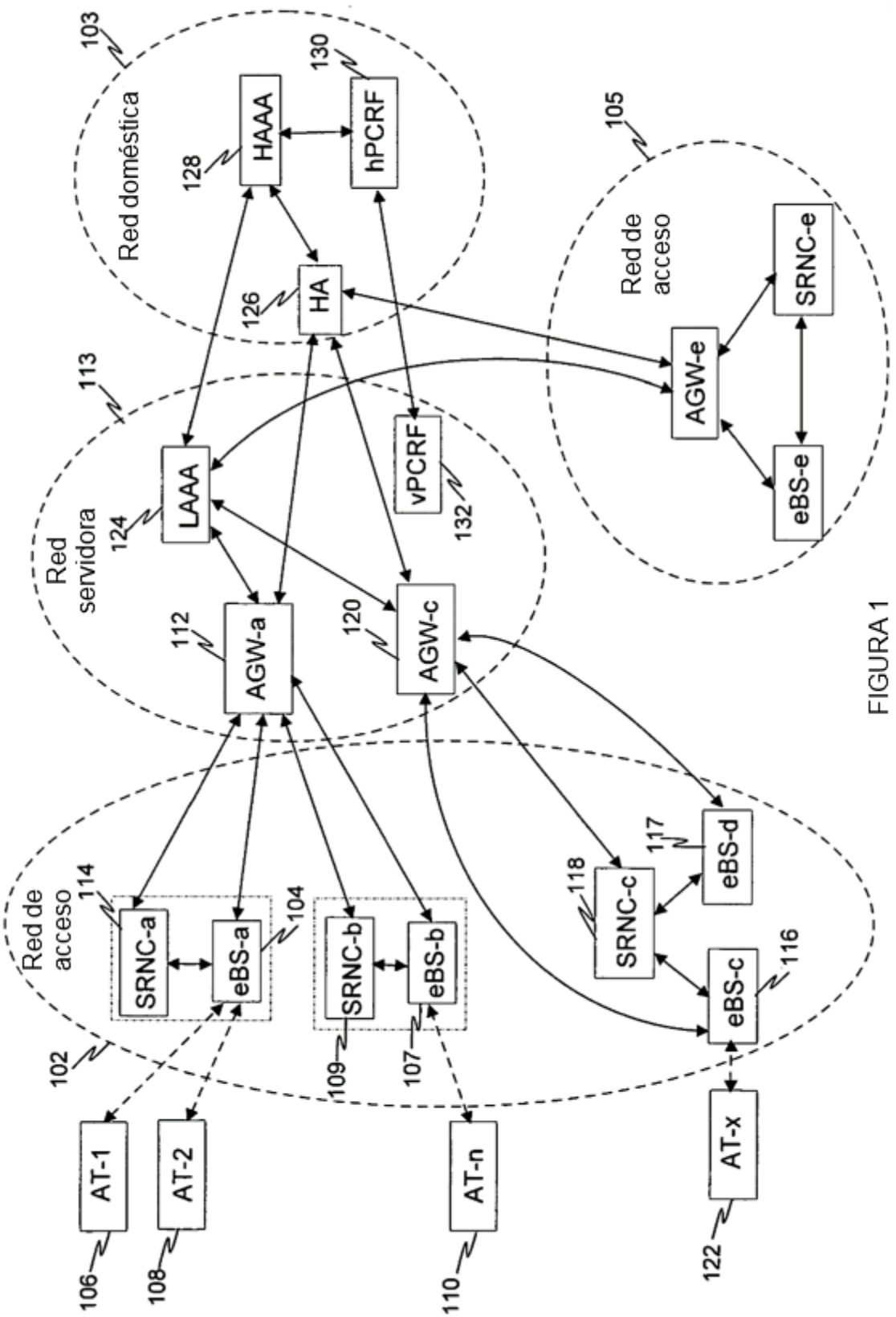
103
Red doméstica
130
hPCRF
128
HAAA
126
HA
105
Red de acceso
SRNC-e
AGW-e
eBS-e
113
Red servidora
LAAA
124
vPCRF
132
112
AGW-a
120
AGW-c
Red de acceso
114
SRNC-a
eBS-a
104
SRNC-b
eBS-b
118
SRNC-c
117
eBS-d
eBS-c
116
102
109
107
AT-1
AT-2
AT-n
AT-x
106
108
110
122

FIGURA 1

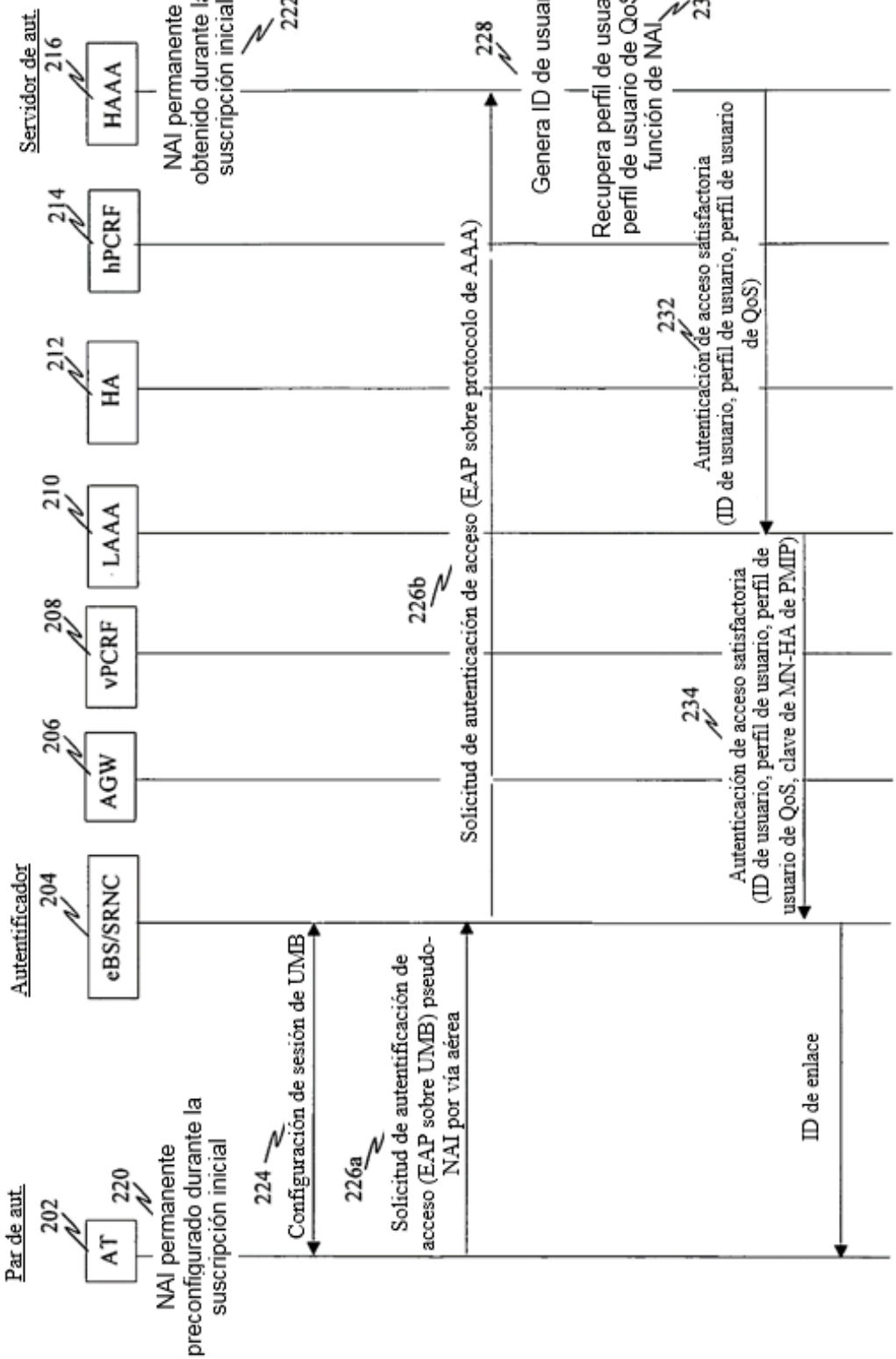
Par de aut.
202
AT
220
NAI permanente preconfigurado durante la suscripción inicial
Autentificador
204
eBS/SRNC
206
AGW
208
vPCRF
210
LAAA
212
HA
214
hPCRF
Servidor de aut.
216
HAAA
NAI permanente obtenido durante la suscripción inicial
222
224
Configuración de sesión de UMB
226a
Solicitud de autentificación de acceso (EAP sobre UMB) pseudo-NAI por vía aérea
226b
Solicitud de autenticación de acceso (EAP sobre protocolo de AAA)
228
Genera ID de usuario
Recupera perfil de usuario y perfil de usuario de QoS en función de NAI
230
232
Autenticación de acceso satisfactoria (ID de usuario, perfil de usuario, perfil de usuario de QoS)
234
Autenticación de acceso satisfactoria (ID de usuario, perfil de usuario, perfil de usuario de QoS, clave de MN-HA de PMIP)
ID de enlace

FIGURA 2

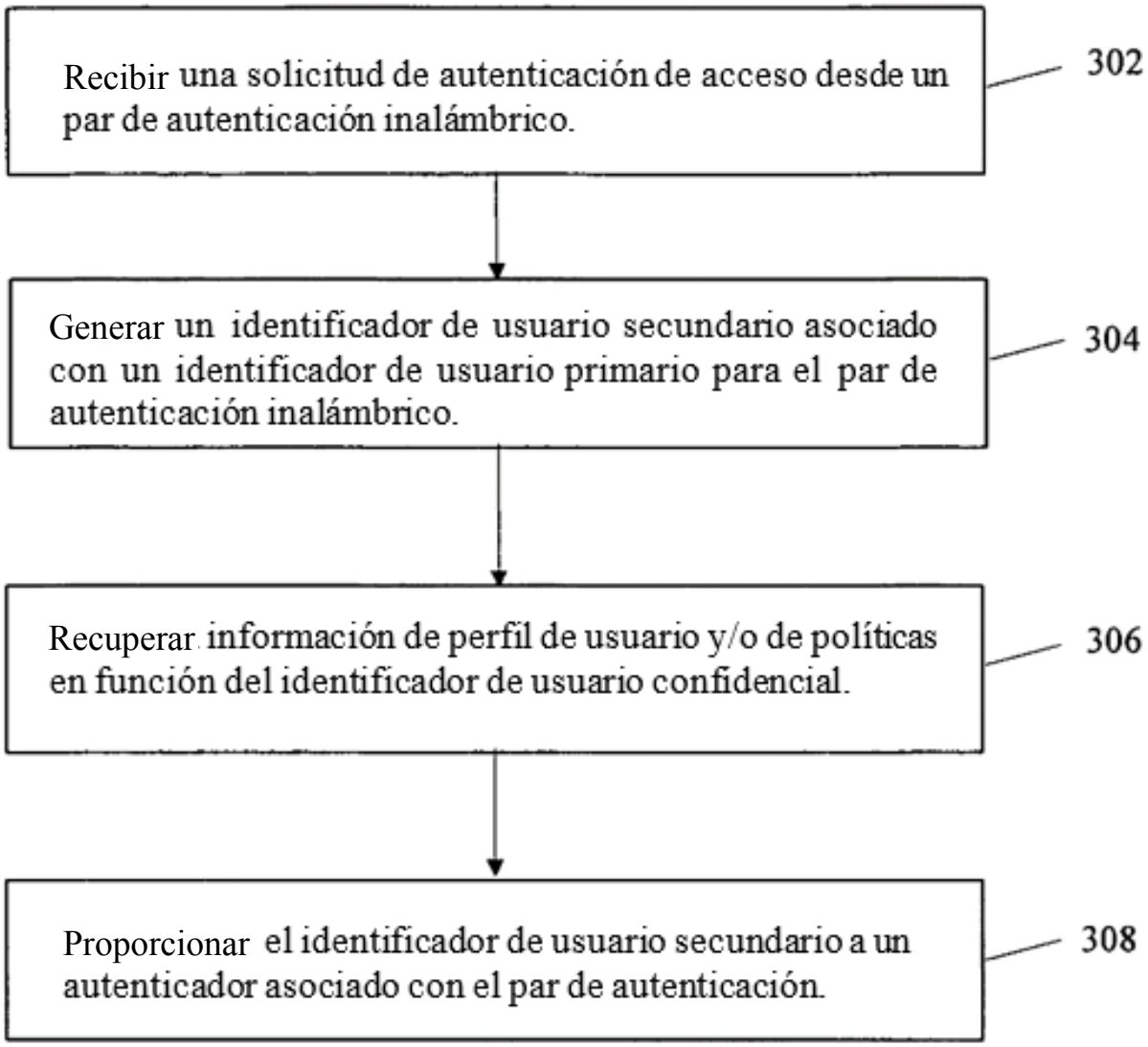
Recibir una solicitud de autenticación de acceso desde un par de autenticación inalámbrico.
302
Generar un identificador de usuario secundario asociado con un identificador de usuario primario para el par de autenticación inalámbrico.
304
Recuperar información de perfil de usuario y/o de políticas en función del identificador de usuario confidencial.
306
Proporcionar el identificador de usuario secundario a un autenticador asociado con el par de autenticación.
308

FIGURA 3

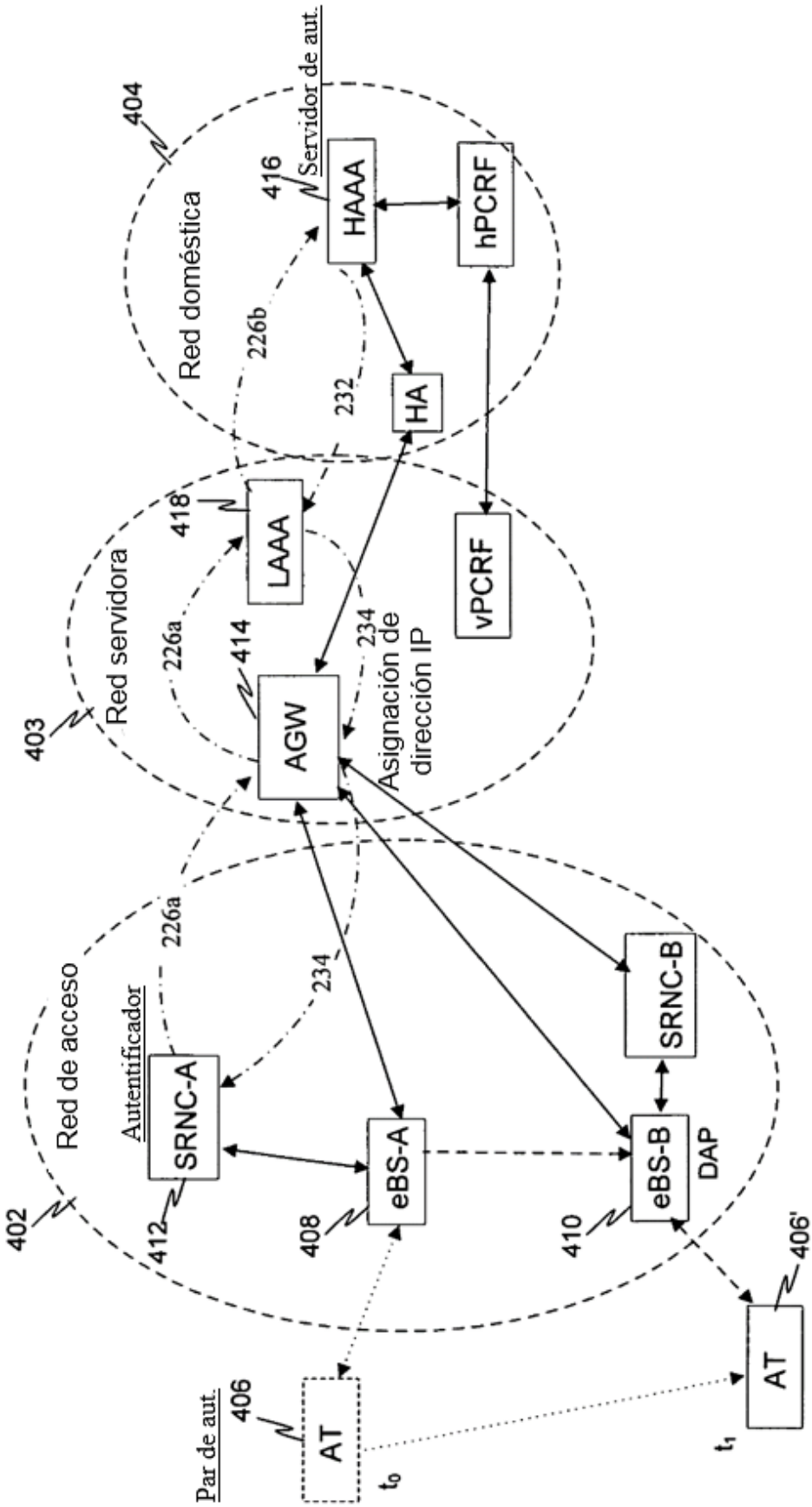
Par de aut.
406
AT
t_0
t_1
AT
406'
402
Red de acceso
Autentificador
SRNC-A
412
eBS-A
408
eBS-B
410
DAP
SRNC-B
226a
234
403
Red servidora
LAAA
418
226a
414
AGW
234
Asignación de dirección IP
vPCRF
404
Red doméstica
226b
232
HA
416
Servidor de aut.
HAAA
hPCRF

FIGURA 4

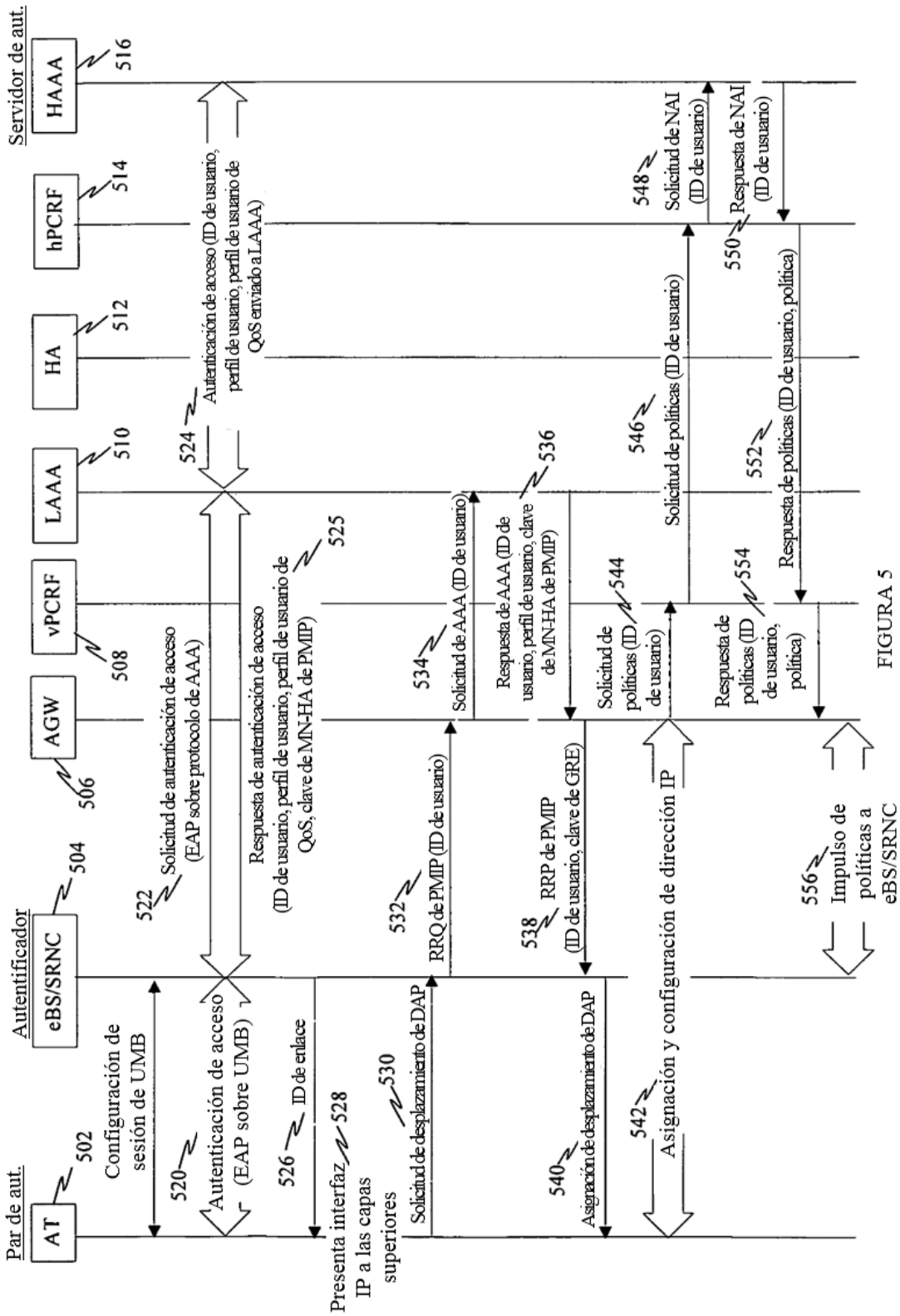
Par de aut.
AT
502
Autentificador
eBS/SRNC
504
AGW
506
vPCRF
508
LAAA
510
HA
512
hPCRF
514
Servidor de aut.
HAAA
516
Configuración de sesión de UMB
520
Autenticación de acceso (EAP sobre UMB)
522
Solicitud de autenticación de acceso (EAP sobre protocolo de AAA)
524
Autenticación de acceso (ID de usuario, perfil de usuario, perfil de usuario de QoS enviado a LAAA)
525
Respuesta de autenticación de acceso (ID de usuario, perfil de usuario, perfil de usuario de QoS, clave de MN-HA de PMIP)
526
ID de enlace
528
Presenta interfaz IP a las capas superiores
530
Solicitud de desplazamiento de DAP
532
RRQ de PMIP (ID de usuario)
534
Solicitud de AAA (ID de usuario)
536
Respuesta de AAA (ID de usuario, perfil de usuario, clave de MN-HA de PMIP)
538
RRP de PMIP (ID de usuario, clave de GRE)
540
Asignación de desplazamiento de DAP
542
Asignación y configuración de dirección IP
544
Solicitud de políticas (ID de usuario)
546
Solicitud de políticas (ID de usuario)
548
Solicitud de NAI (ID de usuario)
550
Respuesta de NAI (ID de usuario)
552
Respuesta de políticas (ID de usuario, política)
554
Respuesta de políticas (ID de usuario, política)
556
Impulso de políticas a eBS/SRNC

FIGURA 5

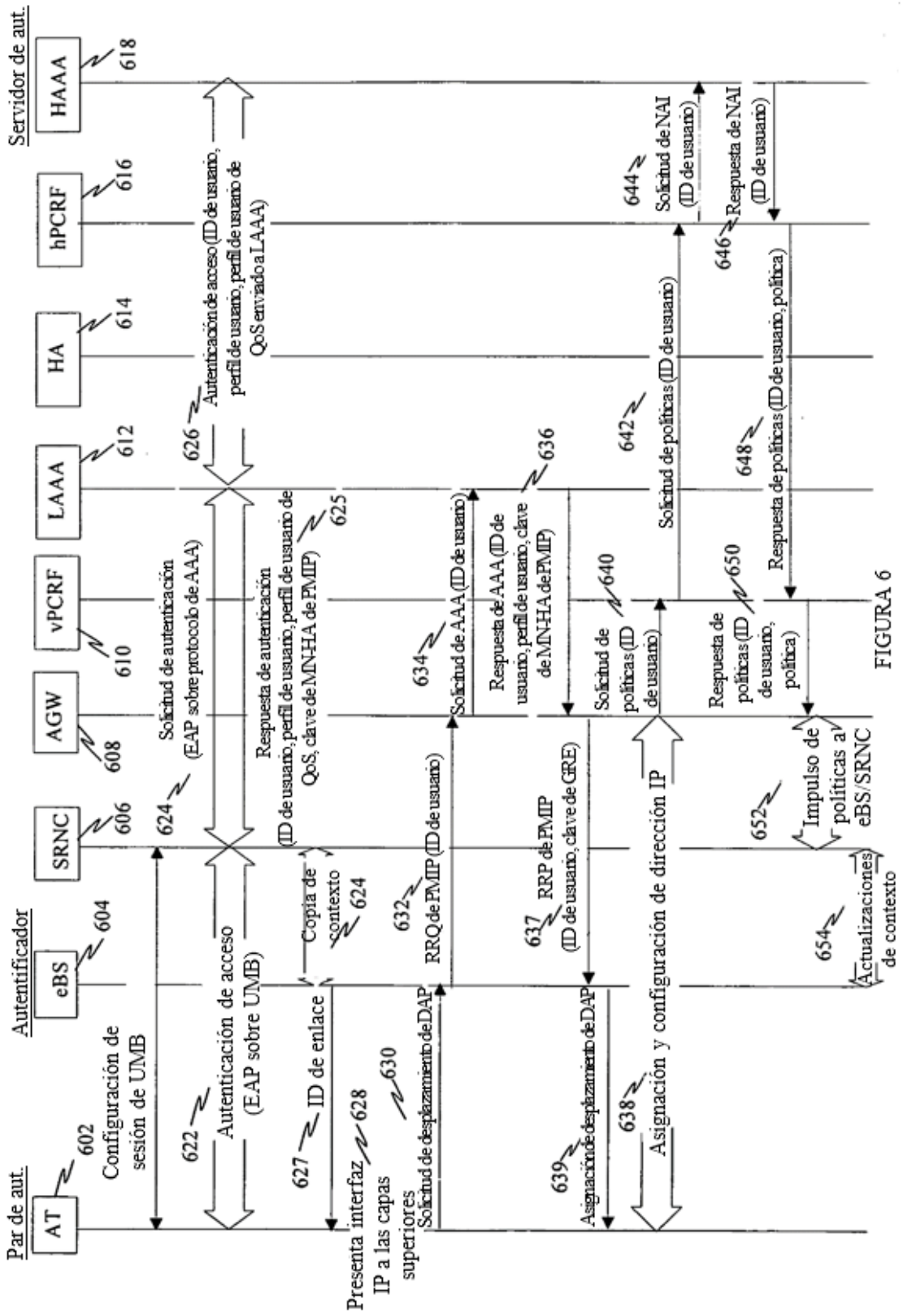
Par de aut.
Autentificador
Servidor de aut.
AT
eBS
SRNC
AGW
vPCRF
LAAA
HA
hPCRF
HAAA
602
604
606
608
610
612
614
616
618
Configuración de sesión de UMB
622
Autenticación de acceso (EAP sobre UMB)
624
Solicitud de autenticación (EAP sobre protocolo de AAA)
626
Autenticación de acceso (ID de usuario, perfil de usuario, perfil de usuario de QoS enviado a LAAA)
627
ID de enlace
Copia de contexto 624
625
Respuesta de autenticación (ID de usuario, perfil de usuario, perfil de usuario de QoS, clave de MN-HA de PMIP)
Presenta interfaz IP a las capas superiores
628
630
Solicitud de desplazamiento de DAP
632
RRQ de PMIP (ID de usuario)
634
Solicitud de AAA (ID de usuario)
636
Respuesta de AAA (ID de usuario, perfil de usuario, clave de MN-HA de PMIP)
637
RRP de PMIP (ID de usuario, clave de GRE)
638
Asignación y configuración de dirección IP
639
Asignación de desplazamiento de DAP
640
Solicitud de políticas (ID de usuario)
642
Solicitud de políticas (ID de usuario)
644
Solicitud de NAI (ID de usuario)
646
Respuesta de NAI (ID de usuario)
648
Respuesta de políticas (ID de usuario, política)
650
Respuesta de políticas (ID de usuario, política)
652
Impulso de políticas a eBS/SRNC
654
Actualizaciones de contexto

FIGURA 6

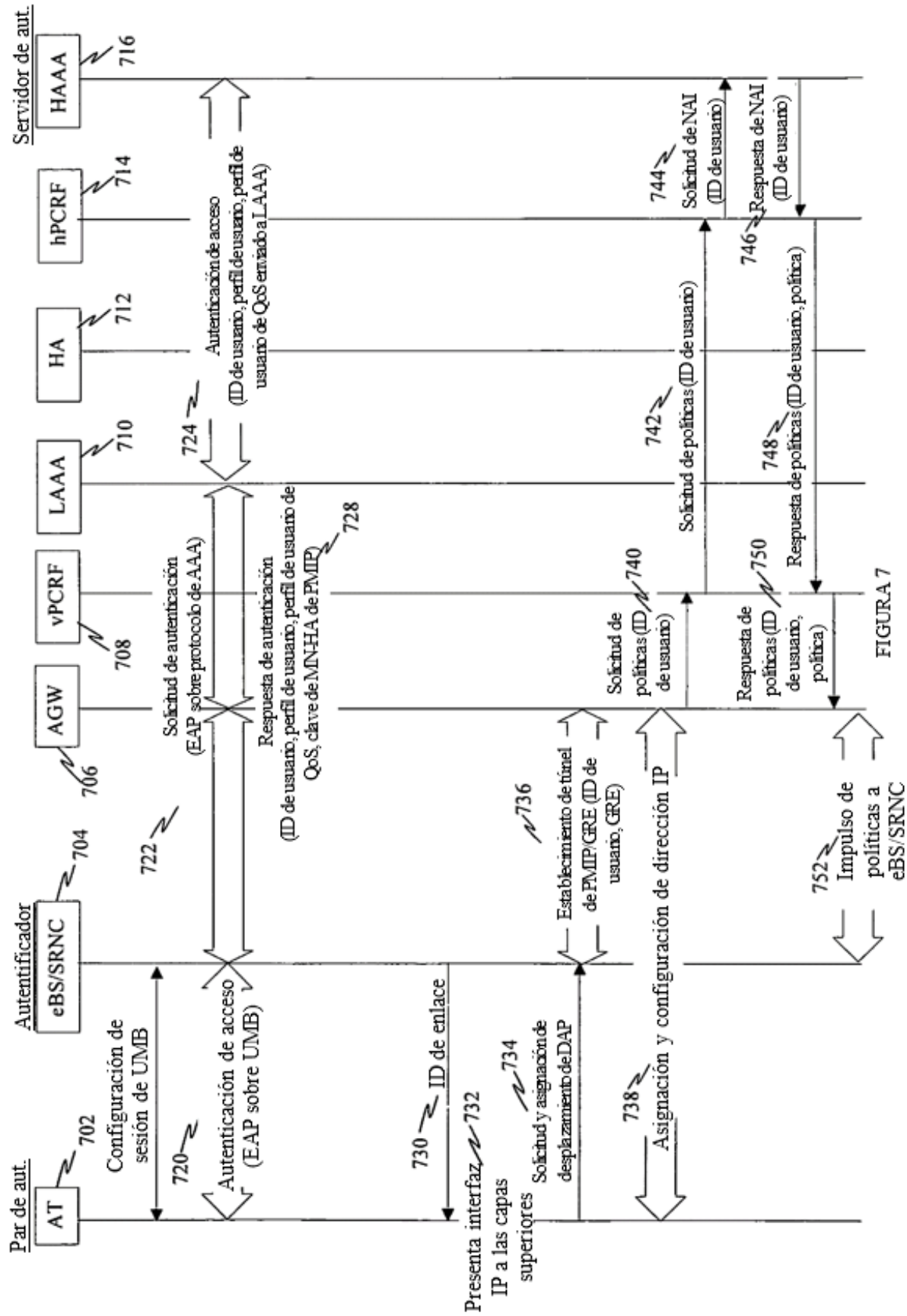
Par de aut.
AT
702
Autentificador
eBS/SRNC
704
AGW
706
vPCRF
708
LAAA
710
HA
712
hPCRF
714
Servidor de aut.
HAAA
716
Configuración de sesión de UMB
720
Autenticación de acceso (EAP sobre UMB)
722
Solicitud de autenticación (EAP sobre protocolo de AAA)
724
Autenticación de acceso (ID de usuario, perfil de usuario, perfil de usuario de QoS enviado a LAAA)
Respuesta de autenticación (ID de usuario, perfil de usuario, perfil de usuario de QoS, clave de MN-HA de PMIP)
728
730
ID de enlace
732
Presenta interfaz IP a las capas superiores
734
Solicitud y asignación de desplazamiento de DAP
736
Establecimiento de túnel de PMIP/GRE (ID de usuario, GRE)
738
Asignación y configuración de dirección IP
740
Solicitud de políticas (ID de usuario)
742
Solicitud de políticas (ID de usuario)
744
Solicitud de NAI (ID de usuario)
746
Respuesta de NAI (ID de usuario)
748
Respuesta de políticas (ID de usuario, política)
750
Respuesta de políticas (ID de usuario, política)
752
Impulso de políticas a eBS/SRNC

FIGURA 7

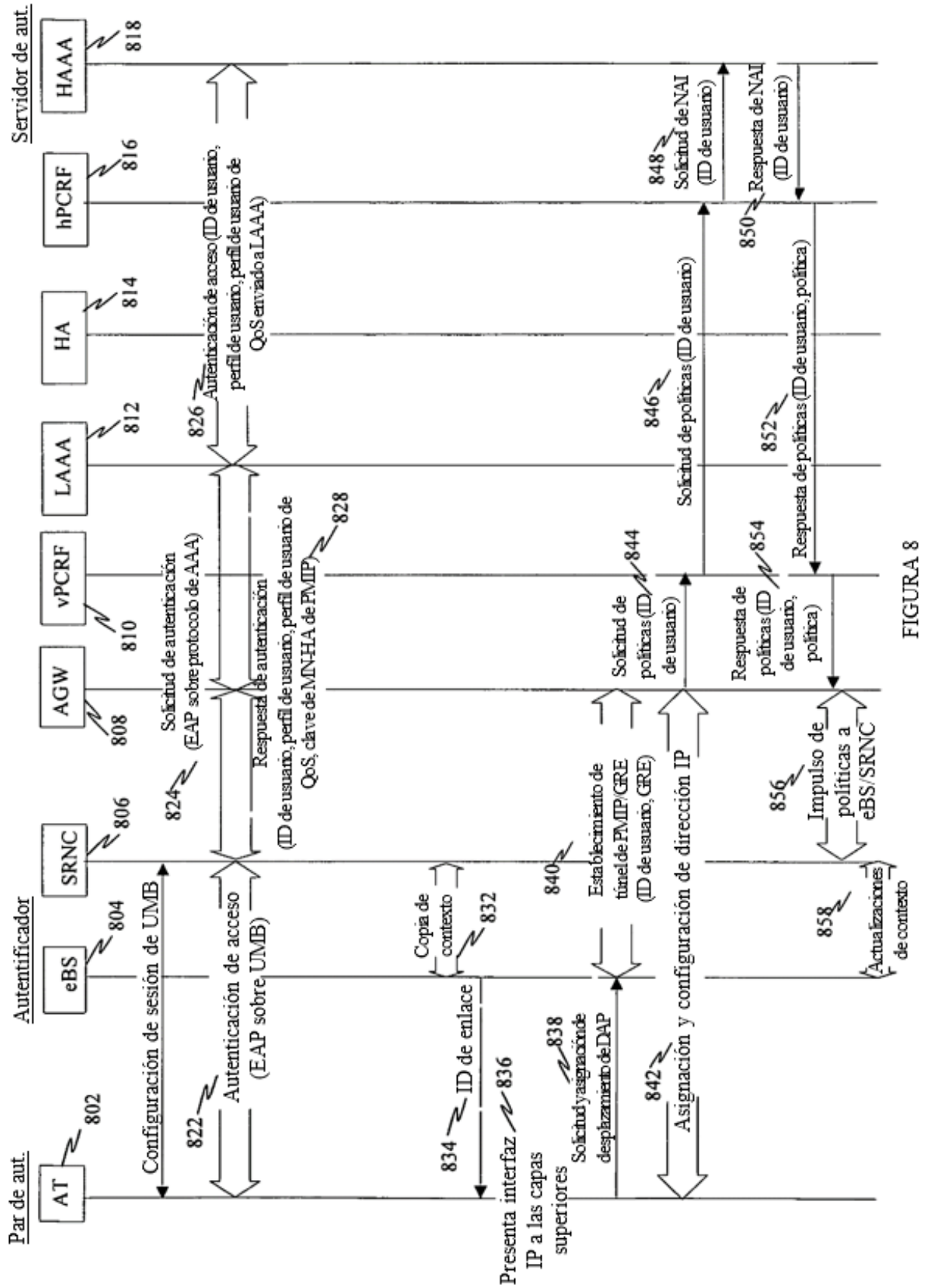
Par de aut.
Autentificador
Servidor de aut.
AT
802
eBS
804
SRNC
806
AGW
808
vPCRF
810
LAAA
812
HA
814
hPCRF
816
HAAA
818
Configuración de sesión de UMB
Autenticación de acceso (EAP sobre UMB)
822
Solicitud de autenticación (EAP sobre protocolo de AAA)
824
826
Autenticación de acceso (ID de usuario, perfil de usuario, perfil de usuario de QoS enviado a LAAA)
Respuesta de autenticación (ID de usuario, perfil de usuario, perfil de usuario de QoS, clave de MN-HA de PMIP)
828
Copia de contexto
832
ID de enlace
834
836
Presenta interfaz IP a las capas superiores
Solicitud y asignación de desplazamiento de DAP
838
840
Establecimiento de túnel de PMIP/GRE (ID de usuario, GRE)
Solicitud de políticas (ID de usuario)
844
Asignación y configuración de dirección IP
842
Solicitud de políticas (ID de usuario)
846
Solicitud de NAI (ID de usuario)
848
Respuesta de NAI (ID de usuario)
850
Respuesta de políticas (ID de usuario, política)
852
Respuesta de políticas (ID de usuario, política)
854
Impulso de políticas a eBS/SRNC
856
Actualizaciones de contexto
858

FIGURA 8

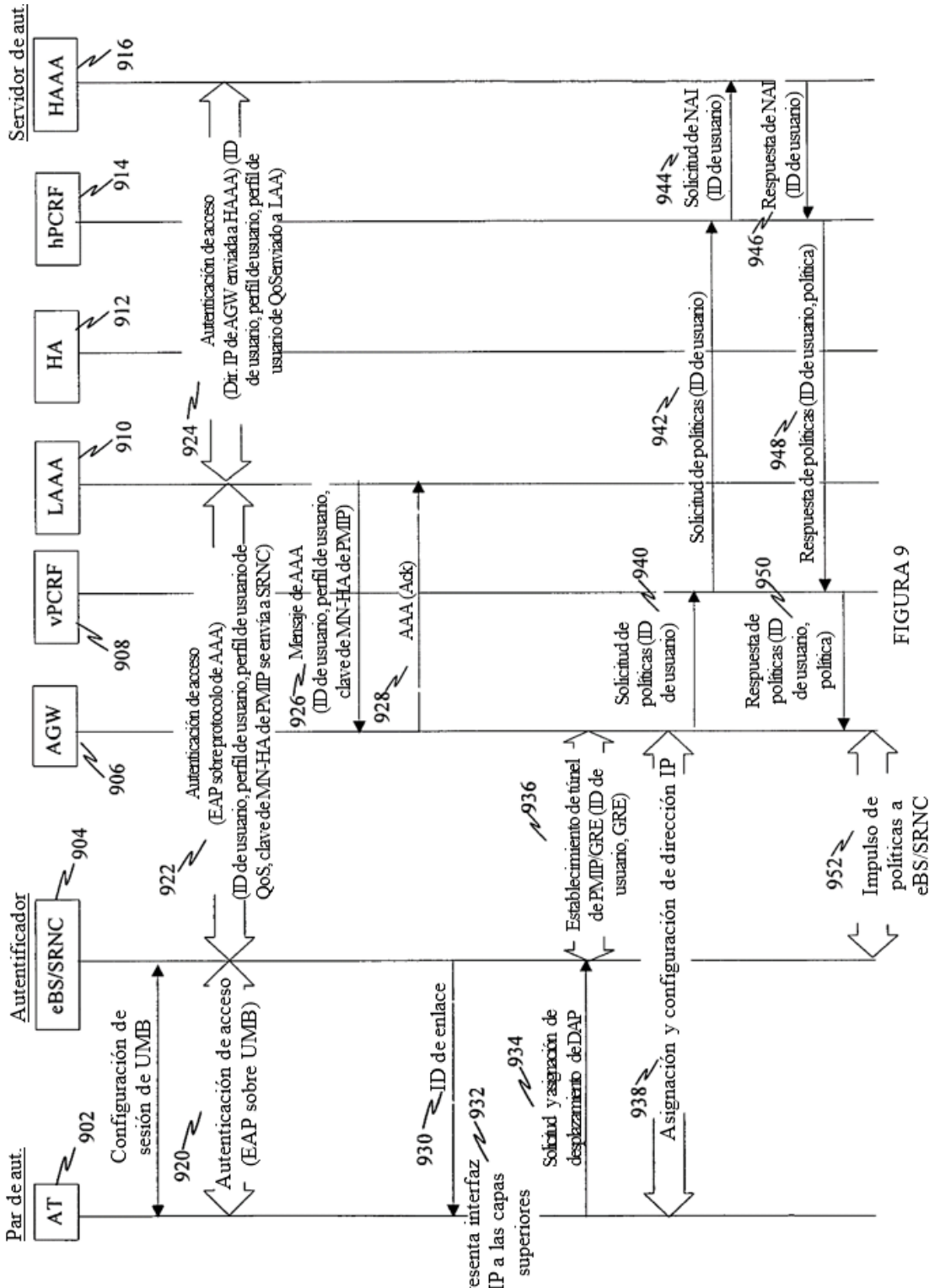
Par de aut.
AT
902
Autentificador
eBS/SRNC
904
AGW
906
vPCRF
908
LAAA
910
HA
912
hPCRF
914
Servidor de aut.
HAAA
916
Configuración de sesión de UMB
920
Autenticación de acceso (EAP sobre UMB)
922
Autenticación de acceso (EAP sobre protocolo de AAA)
(ID de usuario, perfil de usuario, perfil de usuario de QoS, clave de MN-HA de PMIP se envía a SRNC)
924
Autenticación de acceso (Dir. IP de AGW enviada a HAAA) (ID de usuario, perfil de usuario, perfil de usuario de QoServicio a LAA)
926
Mensaje de AAA (ID de usuario, perfil de usuario, clave de MN-HA de PMIP)
928
AAA (Ack)
930
ID de enlace
932
Presenta interfaz IP a las capas superiores
934
Solicitud y asignación de desplazamiento de DAP
936
Establecimiento de túnel de PMIP/GRE (ID de usuario, GRE)
938
Asignación y configuración de dirección IP
940
Solicitud de políticas (ID de usuario)
942
Solicitud de políticas (ID de usuario)
944
Solicitud de NAI (ID de usuario)
946
Respuesta de NAI (ID de usuario)
948
Respuesta de políticas (ID de usuario, política)
950
Respuesta de políticas (ID de usuario, política)
952
Impulso de políticas a eBS/SRNC

FIGURA 9

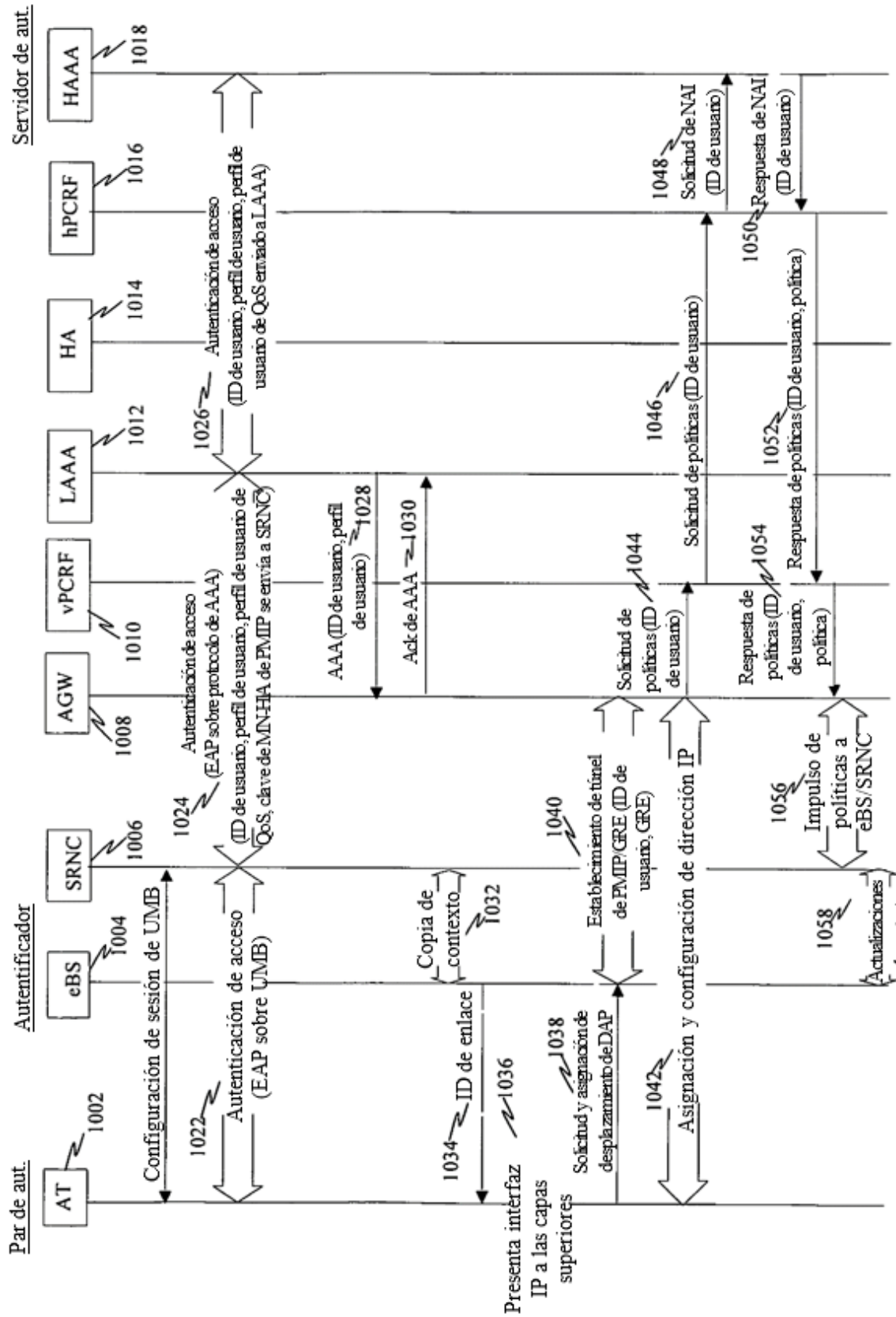
Par de aut.
Autentificador
Servidor de aut.
AT
1002
eBS
1004
SRNC
1006
AGW
1008
vPCRF
1010
LAAA
1012
HA
1014
hPCRF
1016
HAAA
1018
Configuración de sesión de UMB
Autenticación de acceso (EAP sobre UMB)
1022
Autenticación de acceso (EAP sobre protocolo de AAA)
1024
(ID de usuario, perfil de usuario, perfil de usuario de QoS, clave de MN-HA de PMIP se envía a SRNC)
1026
Autenticación de acceso (ID de usuario, perfil de usuario, perfil de usuario de QoS enviado a LAAA)
AAA (ID de usuario, perfil de usuario)
1028
Ack de AAA
1030
Copia de contexto
1032
ID de enlace
1034
Presenta interfaz IP a las capas superiores
1036
Solicitud y asignación de desplazamiento de DAP
1038
Establecimiento de túnel de PMIP/GRE (ID de usuario, GRE)
1040
Asignación y configuración de dirección IP
1042
Solicitud de políticas (ID de usuario)
1044
Solicitud de políticas (ID de usuario)
1046
Solicitud de NAI (ID de usuario)
1048
Respuesta de NAI (ID de usuario)
1050
Respuesta de políticas (ID de usuario, política)
1052
Respuesta de políticas (ID de usuario, política)
1054
Impulso de políticas a eBS/SRNC
1056
Actualizaciones de contexto
1058

FIGURA 10

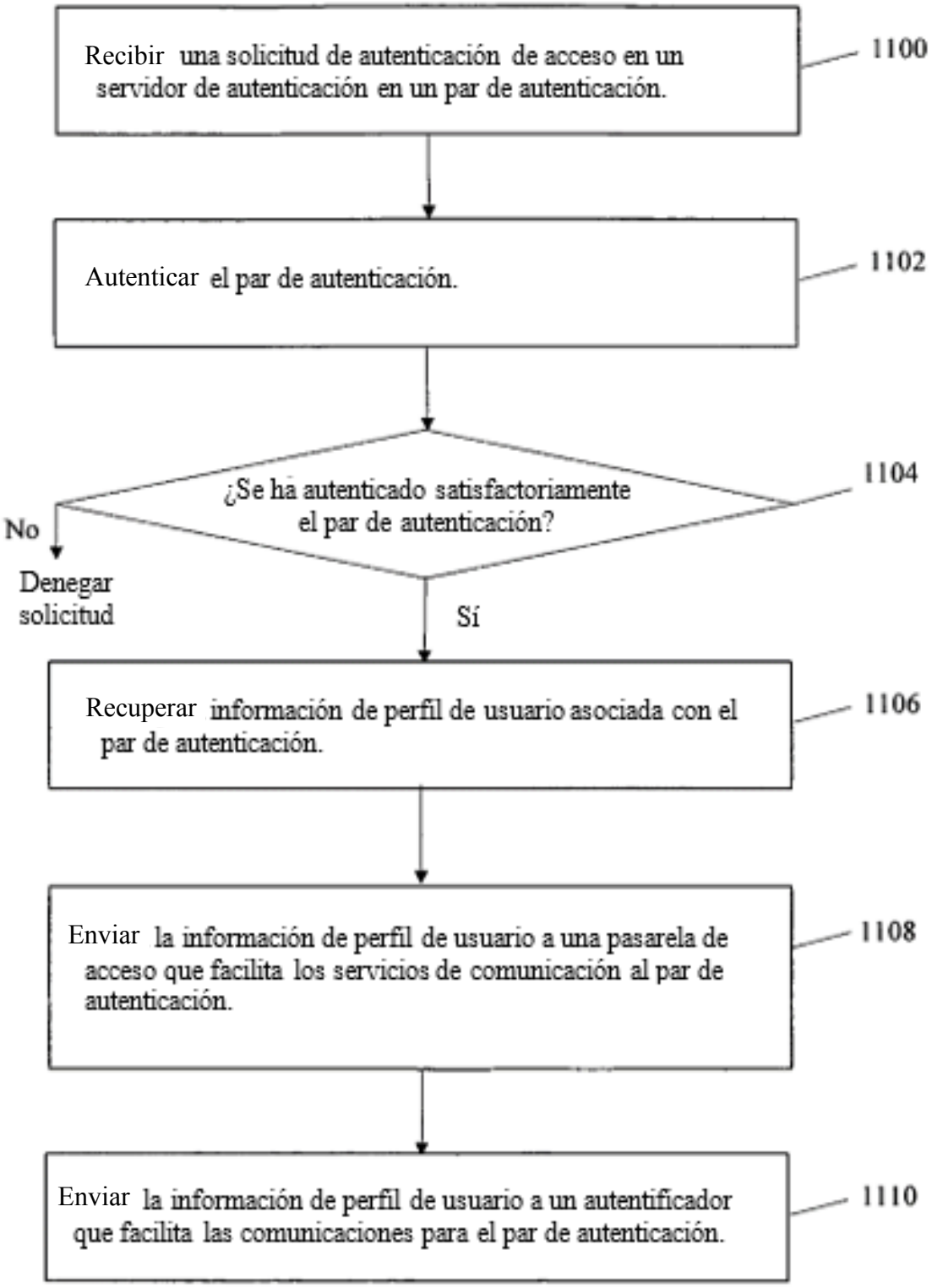
Recibir una solicitud de autenticación de acceso en un servidor de autenticación en un par de autenticación.
1100
Autenticar el par de autenticación.
1102
¿Se ha autenticado satisfactoriamente el par de autenticación?
1104
No
Denegar solicitud
Sí
Recuperar información de perfil de usuario asociada con el par de autenticación.
1106
Enviar la información de perfil de usuario a una pasarela de acceso que facilita los servicios de comunicación al par de autenticación.
1108
Enviar la información de perfil de usuario a un autentificador que facilita las comunicaciones para el par de autenticación.
1110

FIGURA 11

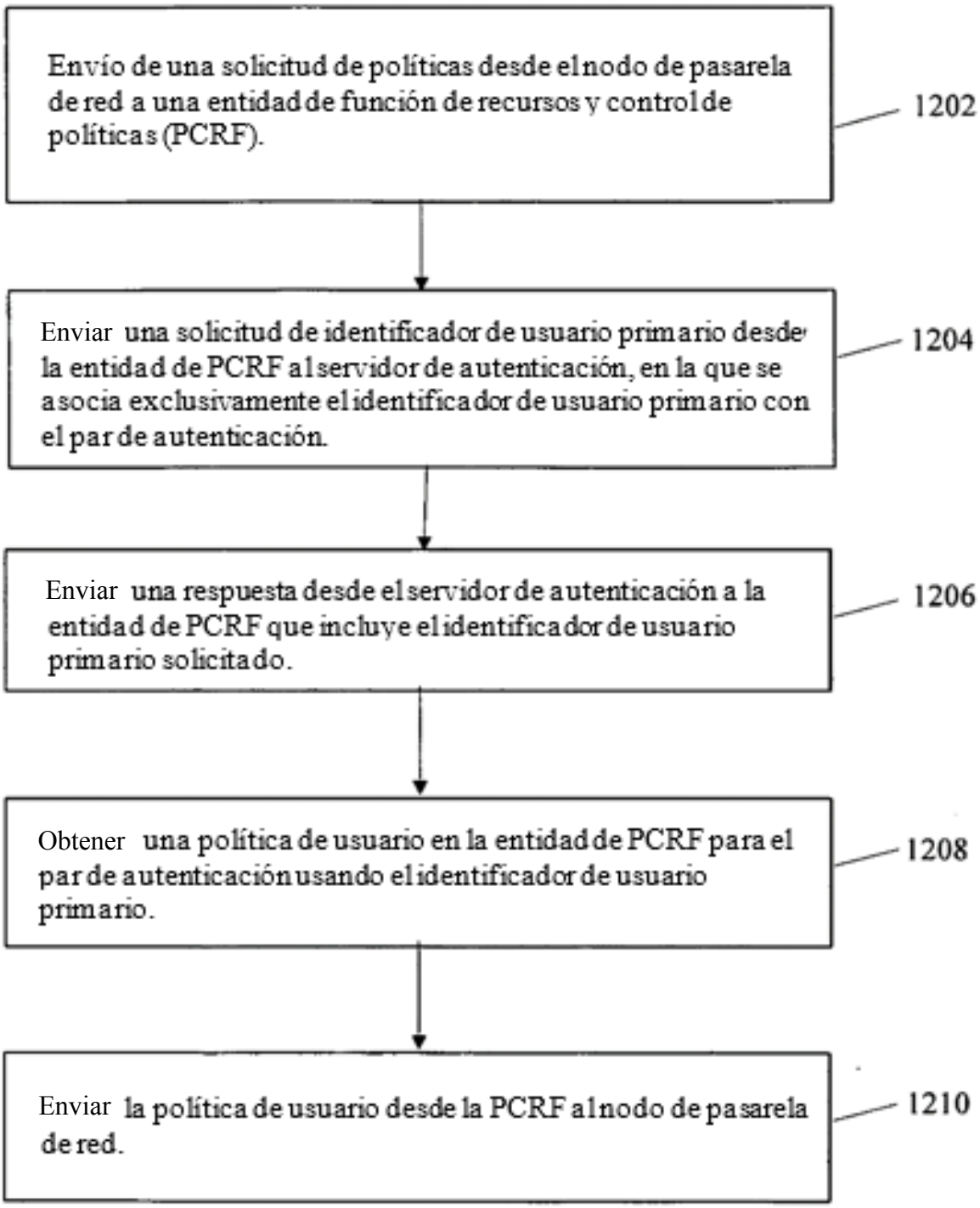
Envío de una solicitud de políticas desde el nodo de pasarela de red a una entidad de función de recursos y control de políticas (PCRF).
1202
Enviar una solicitud de identificador de usuario primario desde la entidad de PCRF al servidor de autenticación, en la que se asocia exclusivamente el identificador de usuario primario con el par de autenticación.
1204
Enviar una respuesta desde el servidor de autenticación a la entidad de PCRF que incluye el identificador de usuario primario solicitado.
1206
Obtener una política de usuario en la entidad de PCRF para el par de autenticación usando el identificador de usuario primario.
1208
Enviar la política de usuario desde la PCRF al nodo de pasarela de red.
1210

FIGURA 12

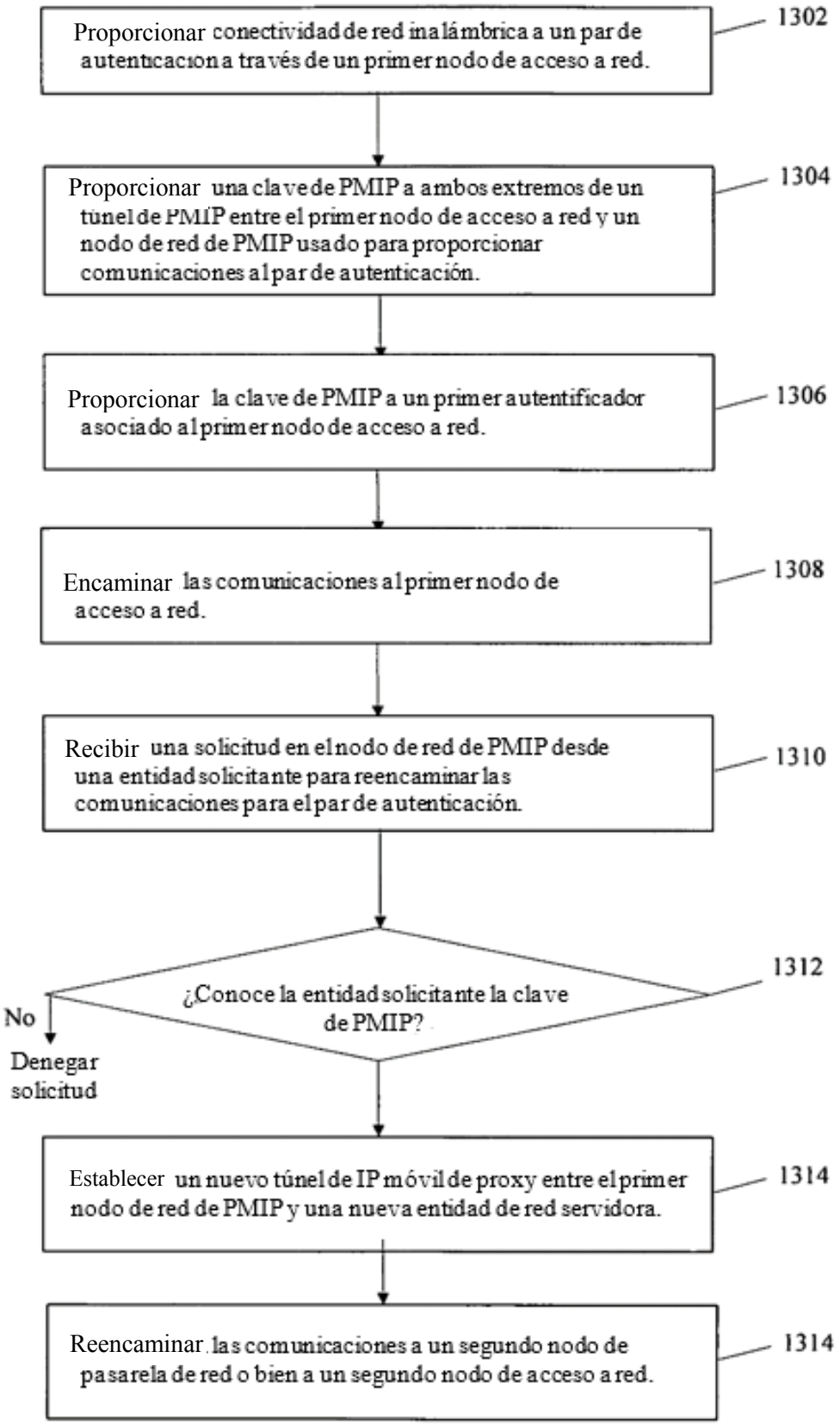
Proporcionar conectividad de red inalámbrica a un par de autenticacion a través de un primer nodo de acceso a red.
1302
Proporcionar una clave de PMIP a ambos extremos de un túnel de PMIP entre el primer nodo de acceso a red y un nodo de red de PMIP usado para proporcionar comunicaciones al par de autenticación.
1304
Proporcionar la clave de PMIP a un primer autentificador asociado al primer nodo de acceso a red.
1306
Encaminar las comunicaciones al primer nodo de acceso a red.
1308
Recibir una solicitud en el nodo de red de PMIP desde una entidad solicitante para reencaminar las comunicaciones para el par de autenticación.
1310
¿Conoce la entidad solicitante la clave de PMIP?
1312
No
Denegar solicitud
Establecer un nuevo túnel de IP móvil de proxy entre el primer nodo de red de PMIP y una nueva entidad de red servidora.
1314
Reencaminar las comunicaciones a un segundo nodo de pasarela de red o bien a un segundo nodo de acceso a red.
1314

FIGURA 13

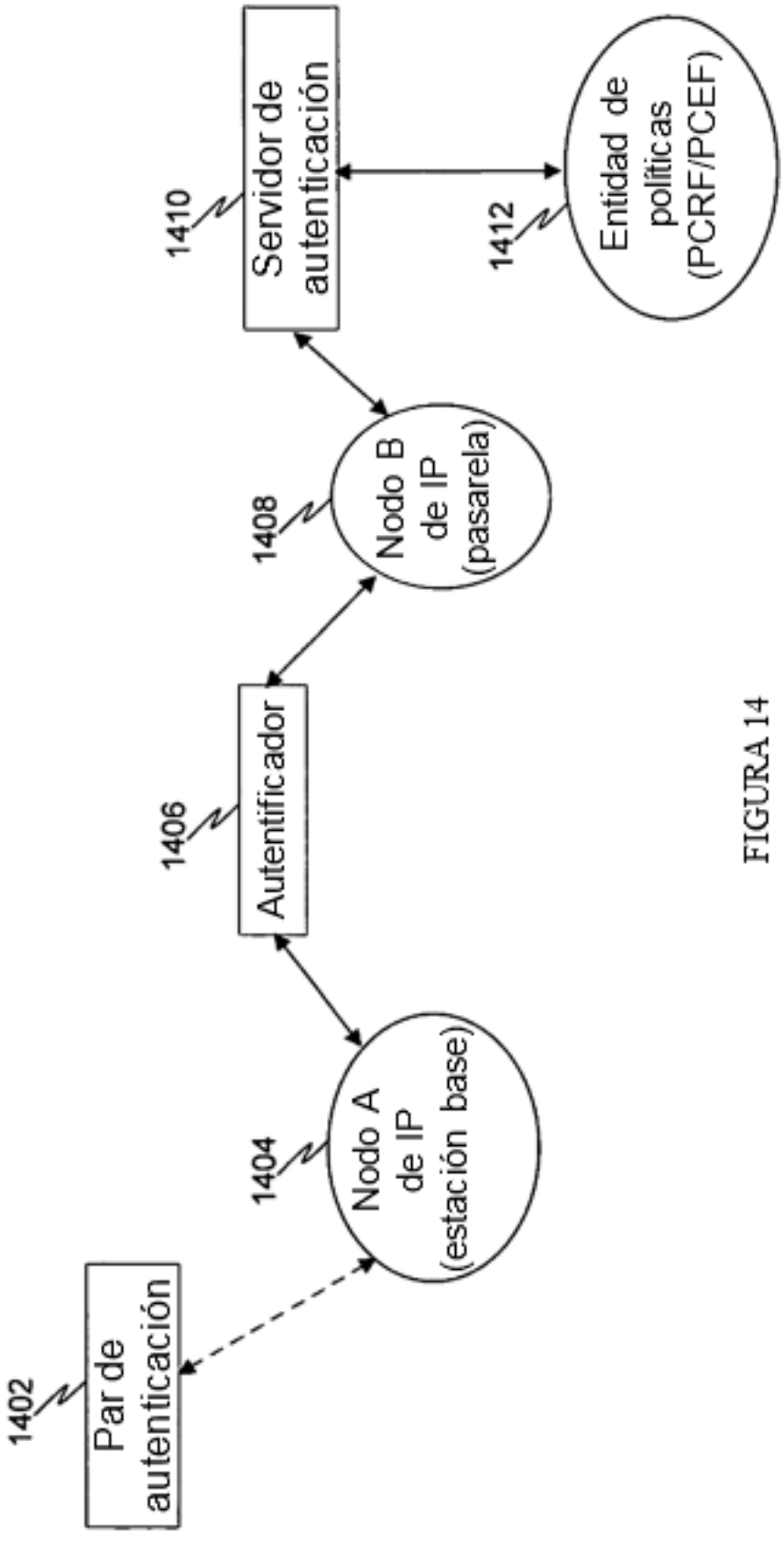
1402
Par de autenticación
1404
Nodo A de IP (estación base)
1406
Autentificador
1408
Nodo B de IP (pasarela)
1410
Servidor de autenticación
1412
Entidad de políticas (PCRF/PCEF)

FIGURA 14

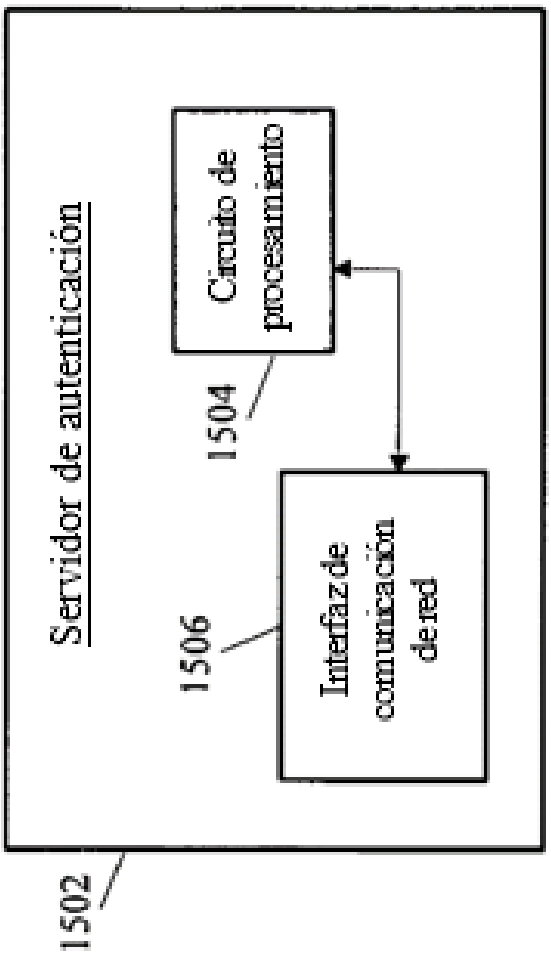
Servidor de autenticación
Circuito de procesamiento
1504
Interfaz de comunicación de red
1506
1502

FIGURA 15

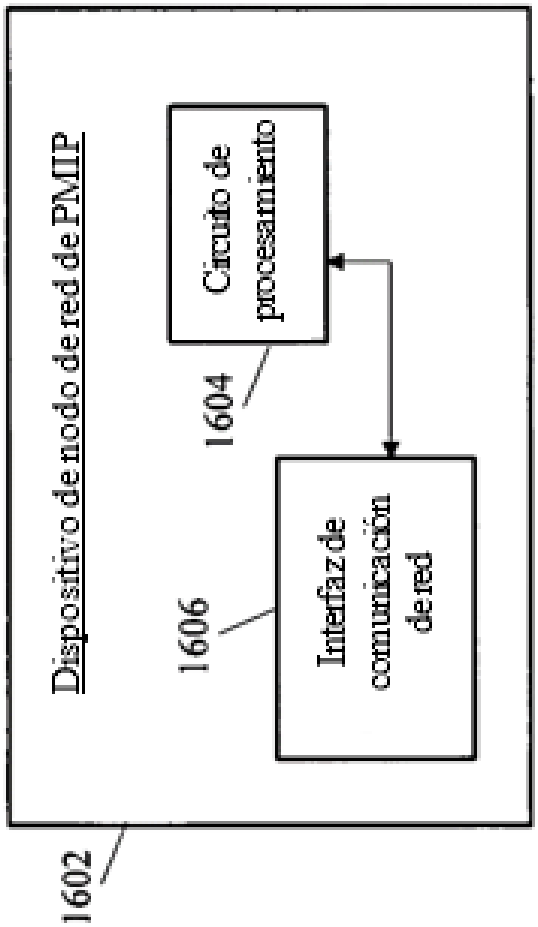
Dispositivo de nodo de red de PMIP
Circuito de procesamiento
1604
Interfaz de comunicación de red
1606
1602

FIGURA 16