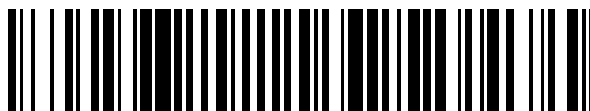


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 401 544**

51 Int. Cl.:

H04W 8/12 (2009.01)

H04L 29/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **30.09.2004 E 10012361 (1)**

97 Fecha y número de publicación de la concesión europea: **19.12.2012 EP 2341723**

54 Título: **Control de la movilidad de un terminal móvil en una red de comunicaciones**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
22.04.2013

73 Titular/es:

TELECOM ITALIA S.P.A. (100.0%)
Piazza degli Affari 2
20123 Milano, IT

72 Inventor/es:

GIARETTA, GERARDO y
GUARDINI, IVANO

74 Agente/Representante:

PONTI SALES, Adelaida

ES 2 401 544 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Control de la movilidad de un terminal móvil en una red de comunicaciones.

Campo de la invención

[0001] La presente invención se refiere a técnicas para gestionar el tráfico en redes de telecomunicaciones.

5 **[0002]** La invención se ha desarrollado prestando especial atención a la posible aplicación en redes móviles basadas en IP (Protocolo de Internet), es decir, de una manera más precisa, en redes donde se gestiona la movilidad del terminal con el protocolo IP móvil.

[0003] En cualquier caso, la referencia a este campo particular de aplicación no debe interpretarse en un sentido limitativo para el alcance de la invención.

10 Descripción de la técnica anterior

[0004] Las redes IP móviles identifican un escenario en el que un usuario se mueve dentro de la red y genera el tráfico que se dirige dentro de la red hacia los nodos (los nodos correspondientes) con los que el usuario se está comunicando.

15 **[0005]** Durante sus movimientos, el usuario puede tener que cambiar la red de acceso (sub-red) que le permite utilizar los servicios IP. Esta operación debe ser transparente para el usuario, de manera que pueda estar en comunicación con los nodos correspondientes, sin interrupciones.

20 **[0006]** Los protocolos tradicionales en los que se basan las redes IP, debido a su naturaleza, no son capaces de gestionar terminales IP en movimiento dentro de la red. Para llenar este vacío, el organismo de normalización IETF ("Internet Engineering Task Force") ha definido el protocolo Mobile IPv6, que permite a los terminales móviles IPv6 cambiar su punto de conexión a la red de forma transparente respecto a las aplicaciones.

25 **[0007]** El protocolo IPv6 Móvil se especifica en el documento rfc3775. Esta es la primera de las diferentes referencias hechas en la presente descripción de los estándares o normas del proyecto de tipo borrador-... o rfc...: su información relacionada está disponible para el público en la fecha de presentación de la presente solicitud en el sitio web de la IETF en la dirección <http://www.ietf.org> o, alternativamente, en la base de datos en línea <http://www.watersprings.org>.

30 **[0008]** En caso de que se adopte el protocolo Ipv6 Móvil, dos direcciones IP se asignan al nodo móvil. La primera dirección es la Dirección local (HoA): esta dirección nunca cambia y se utiliza para identificar unívocamente la identidad del nodo (aquí a continuación también llamado nodo móvil o terminal). La segunda dirección es la llamada dirección de atención (CoA): esta dirección identifica la posición real del terminal de telefonía móvil en la sub-red visitada y luego cambia a cada movimiento de una sub-red a otra.

35 **[0009]** Cada movimiento que implica un cambio de sub-red IP visitada obliga al terminal móvil a grabar su propia Dirección de atención por un servidor, llamado Agente local (HA), que se puede encontrar en la red del proveedor (también llamada "red local"). Cualquier otro terminal IP que intenta comunicarse con el nodo móvil, contacta con el propio nodo móvil usando la Dirección local. A través del enrutamiento IP normal, el tráfico enviado llega al HA, que vuelve a dirigirlo hacia la posición real del nodo móvil, identificado por la dirección de atención. De esta manera, todo el tráfico destinado al nodo móvil se distribuye por el Agente Local hacia la dirección del usuario actual, es decir, la dirección de atención. A continuación, el nodo móvil debe poderse alcanzar de manera constante cualquiera que sea su punto de conexión a la red.

40 **[0010]** La figura 1 muestra un escenario genérico de uso del protocolo IPv6 Móvil dentro de la red IP que aloja un nodo móvil.

45 **[0011]** En particular, en la figura 1 un nodo móvil 10 tiene a su disposición una serie de puntos de acceso 20 que le permiten establecer una conexión con la red 30 de su proveedor y, más en detalle, permitir que se abra una sesión de comunicación, designada con 40, a través de un servidor particular 50 llamado Agente Local. La sesión de comunicación 40 implica, en el ejemplo mostrado, que recibe el tráfico de datos desde un nodo correspondiente, designado con 15. El nodo móvil 10 que se mueve dentro de la red IP está señalado por la flecha 60. El Agente Local 50 garantiza que el tráfico generado por el nodo correspondiente 15 alcanza el nodo móvil 10 cualquiera que sea el punto de conexión actual del nodo móvil.

50 **[0012]** La colocación y nivel de carga del agente local 50 afectan en gran medida el rendimiento experimentado por el terminal móvil, ya que afectan tanto al retraso con el que el nodo móvil recibe el tráfico de datos y la longitud de la pérdida temporal de conectividad (latencia de handoff) que se produce después de cada movimiento desde un punto de acceso a otro.

[0013] Se conoce a partir de GIARETTA, GUARDINI, DEMARIA BOURNELLE, LAURENT-MAKNAVICIUS, "autorización y configuración MIPv6 sobre EAP", Grupo de Trabajo MIP6, Borrador de Internet, 16 de julio 2004

5 [ref. draftgiaretta-MIP6-authorization-eap-00] que es posible asignar dinámicamente al terminal móvil, por ejemplo al encenderlo, un agente local que es capaz de proporcionar un rendimiento óptimo, es decir, un agente local que tiene recursos de procesamiento disponibles suficientes y puede encontrarse lo más cerca posible, en términos de número de saltos IP, hasta el punto terminal móvil de fijación.

[0014] Sin embargo, en el tiempo, el agente local, inicialmente asignado de acuerdo con estos criterios, puede no ser ya capaz de proporcionar un servicio con la calidad adecuada. Por ejemplo, esto podría ocurrir en las siguientes situaciones:

10 - después de movimientos continuos del terminal móvil, es posible que el Agente local termine bastante lejos del punto de conexión actual del propio terminal móvil, lo que provoca un gran aumento de la latencia de transferencia y el retraso de transferencia de tráfico a su destino;

15 - cuando cambia la cantidad de tráfico generado por los terminales móviles que se pueden encontrar en la red, es posible que el Agente local sea sometido a un estado de congestión, con la consiguiente incapacidad de gestionar todos los terminales móviles conectados a la misma.

20 **[0015]** Para resolver este problema, se conoce un acuerdo llamado Protocolo entre agentes locales (HA-HA) WAKINAWA ET AL., "*Inter Home Agents Protocol (HAHA)*", MIP6/NEMO WORKING GROUP, INTERNET DRAFT, 16 de febrero de 2004, páginas 1-19, [[ref. draf-wakikawa-mip6-nemo-haha-01], que permite que el nodo móvil cambie el Agente local que se utiliza en cada momento, teniendo cada vez el aparato que es capaz de garantizar el mejor rendimiento.

25 **[0016]** La arquitectura sobre la que se basa la solución del Protocolo entre agentes locales, que se muestra en la figura 2, establece que el nodo móvil 10 es servido, en lugar de por un solo Agente local 50 (como en el caso que se muestra en la figura 1), por un grupo de Agentes locales 70 dispuestos en la red del operador 30. Todos los agentes locales 70 pertenecientes al mismo grupo periódicamente intercambian mensajes de señalización para sincronizar información acerca de la posición (es decir, la dirección local y la dirección de atención) de los nodos móviles que se pueden encontrar dentro de la red.

30 **[0017]** Debido a este procedimiento de sincronización, los agentes locales que pertenecen al mismo grupo son vistos por el nodo móvil 10 como un solo Agente local "virtual" 80, lo que significa que el nodo móvil 10 se puede mover desde un agente local a otro sin modificar su propia dirección local, es decir, con un mínimo impacto en las comunicaciones actuales.

[0018] Este enfoque, sin embargo, tiene limitaciones que pueden hacer difícil su aplicación, especialmente en el caso de redes de gran tamaño (por ejemplo, grandes proveedores y operadores con un número significativo de agentes locales):

35 - cada agente local se debe configurar manualmente [ref. draft- wakikawa-mip6-nemo-haha-01, página 17] con las direcciones de todos los demás agentes locales pertenecientes al mismo grupo. Esto hace complicada la gestión de servicios y de suministro, especialmente cuando el número de agentes locales que se pueden encontrar en la red es grande;

40 - para permitir que el nodo móvil mantenga la misma Dirección local independientemente del Agente local que se está utilizando en cada momento, los agentes locales que pertenecen al mismo grupo deben intercambiarse, en un modo punto a punto, un alto número de mensajes de señalización, que son necesarios para sincronizar las tablas de unión entre la Dirección local y Dirección de atención. Esto limita la escalabilidad de la disposición, aumentando la pérdida de recursos, tales como, por ejemplo, recursos de ancho de banda en conexiones de red y la carga de computación sobre los agentes locales.

45 **[0019]** Aquí a continuación, para completar, se incluye la documentación de antecedentes, citados como referencia. En su mayoría son estándares IETF y/o documentos de trabajo.

- Soporte de movilidad para IPv6 (rfc3775);
- Soporte de Movilidad IP para IPv4 (rfc3344);
- Auto-configuración de dirección sin estado IPv6 (rfc2462);
- Protocolo de base de diámetro (rfc3588);
- 50 - Intercambio de claves de Internet (rfc2409);

- Protocolo de intercambio de claves de Internet (IKEv2) (draft-ietf-ipsec-ikev2-15)
 - Protocolo de Autenticación Extensible (rfc3748);
 - Marco de gestión de claves EAP (draft-ietf-EAP-keying-03);
 - Autorización y configuración de MIPv6 basada en EAP (draft-giaretta-MIP6-authorization-eap-00);
- 5 - Protocolo de autenticación para IPv6 Móvil (draft-ietf-MIP6-auth-protocol-00)

Objeto y descripción de la invención

[0020] A partir de la descripción anterior de la situación actual, parece que hay una necesidad de definir una técnica que permita modificar en tiempo real, y con un mínimo impacto sobre las comunicaciones actuales, el agente local que se utiliza mediante un terminal móvil.

10 **[0021]** El objeto de la presente invención es satisfacer la necesidad anterior y, en particular, la invención trata con el problema de proporcionar una solución que no tiene los puntos críticos del Protocolo entre agentes locales, y que se pueda utilizar para permitir que el terminal móvil esté siempre servido por un Agente local que sea capaz de proporcionar un rendimiento óptimo, sin causar ninguna interrupción de los servicios al usuario.

15 **[0022]** De acuerdo con la presente invención, este objeto se obtiene mediante un terminal móvil que tiene las características incluidas en reivindicación 1. La presente invención también se refiere a una plataforma de autenticación, autorización y contabilidad (AAA) tal como se reivindica en la reivindicación 3.

[0023] Unas realizaciones según la presente invención, implican, entre otras, las siguientes ventajas:

20 - optimización del rendimiento: la asignación de un Agente local más cercano al nodo móvil permite la optimización del rendimiento experimentado por el usuario, reduciendo la latencia de transferencia y la transferencia de demora de tráfico dirigido a través del Agente local;

25 - equilibrio de la carga: la posibilidad de modificar el Agente local que se utiliza por un determinado usuario permite intervenir en tiempo real en la división de la carga entre los Agentes locales que están presentes en la red, para adaptarla al tipo y a la cantidad de tráfico generado por los usuarios. Por ejemplo, para evitar la ocurrencia de un estado de congestión, es posible disminuir de forma dinámica el nivel de carga de un determinado Agente local haciendo que uno o más nodos móviles sean servidos por otro Agente local;

30 - utilización óptima de los recursos de la red del operador: la asignación de un Agente local más cercano al nodo móvil permite reducir la cantidad de tráfico que atraviesa la red del operador (por ejemplo, la columna central). En particular, esto garantiza un aprovechamiento óptimo de los recursos de red, evitando que el tráfico relacionado con los nodos móviles transite inútilmente a través de las conexiones geográficas que componen la columna central del operador.

Breve descripción de los dibujos

[0024] La invención se describirá ahora, como un ejemplo no limitativo, con referencia a las figuras adjuntas de dibujos, en los que:

- Las figuras 1 y 2 ya han sido descritas previamente;
- 35 - La figura 3 muestra una posible arquitectura de red de la disposición aquí descrita;
- La figura 4 muestra con más detalle la arquitectura de red de la disposición aquí descrita;
- La figura 5 muestra un diagrama de flujo funcional que representa un procedimiento de reasignación del Agente local iniciado por un nodo móvil y que termina con éxito;
- 40 - La figura 6 muestra un diagrama de flujo funcional que representa un procedimiento de reasignación del Agente local solicitado por el nodo móvil, pero rechazado, ya que no fue autorizado;
- La figura 7 muestra un diagrama de flujo funcional que representa un procedimiento de reasignación del Agente local iniciado por el Agente local actualmente utilizado por el nodo móvil y terminado con éxito;
- La figura 8 muestra un diagrama de flujo funcional que representa un procedimiento de reasignación del Agente local iniciado por el servidor AAA y terminado con éxito;
- 45 - La figura 9 muestra un diagrama de flujo funcional que representa un procedimiento de reasignación del Agente local iniciado por el servidor AAA, pero con fallo, ya que estaba relacionado con un nodo móvil que no

soporta el procedimiento;

- La figura 10 muestra el cierre del procedimiento a través de mensajes de contabilidad;
- La figura 11 muestra una posible división en zonas de un operador de red;
- La figura 12 muestra un ejemplo métrico entre las zonas en las que se puede dividir un operador de red;

5 - La figura 13 muestra un posible nuevo formato del mensaje de actualización de la unión que se puede utilizar en el contexto de la disposición aquí descrita;

- La figura 14 muestra el formato genérico de una opción de movilidad que se puede utilizar en el contexto de la disposición aquí descrita;

10 - La figura 15 muestra un posible formato de una opción de movilidad de datos de reasignación del agente local que se puede utilizar en el contexto de la disposición aquí descrita; y

- La figura 16 muestra un posible formato de una opción de movilidad de pistas de reasignación del agente local que se puede utilizar en el contexto de la disposición aquí descrita.

Descripción detallada de las realizaciones de la invención

15 **[0025]** La figura 3 muestra con referencia directa a los diagramas ya mostrados en las figuras 1 y 2, un ejemplo de arquitectura de red en la que se basa la disposición aquí descrita.

20 **[0026]** La arquitectura en la figura 3 prevé el uso de la plataforma de autenticación, autorización y contabilidad (AAA) 90 del proveedor con el que el usuario ha suscrito el servicio. Esto para hacer que dicha plataforma, ya normalmente presente en el proveedor de red 30, autorice, conduzca y supervise todo el proceso de migración hacia un nuevo Agente local (Agente local designado), mediante el envío de comandos de configuración e información a los Agentes locales 70, presentes en la red, y al nodo móvil 10. La comunicación entre la plataforma de Autenticación, Autorización y Contabilidad (AAA) 90 y el nodo móvil 10 se realiza con el soporte del Agente local que actualmente sirve al nodo móvil (es decir, el Agente local de servicio) a través de extensiones adecuadas en el protocolo AAA, designado con 100 en la figura 3, y en mensajes de señalización IPv6 Móvil, designado con 102 en la figura 3.

25 **[0027]** Cada uno de los agentes locales 70 presentes en la red opera así de manera independiente de los otros y gestiona su propio espacio de direccionamiento. En consecuencia, el nodo móvil 10 modifica su propia Dirección local en cada cambio de Agente local. La supervivencia de las sesiones de la aplicación está garantizada proporcionando un período transitorio durante el cual el nodo móvil 10 puede utilizar simultáneamente las direcciones locales antigua y nueva, de manera que las aplicaciones iniciadas antes del inicio del procedimiento de reasignación pueden terminar sin interrupciones.

30 **[0028]** Operando de esta manera, aunque aumentando la complejidad del nodo móvil 10, que debe ser capaz de comunicarse simultáneamente con el Agente local antiguo (de servicio) y el nuevo (designado), no es necesario prever ningún intercambio de información para la coordinación de los agentes locales que están presentes en la red. Se obtiene así un aumento en la escalabilidad del sistema y una reducción de la señalización superior.

35 **[0029]** El protocolo IPv6 Móvil (MIPv6) es la solución propuesta dentro de la IETF ("Internet Engineering Task Force"), para gestionar la movilidad de amplio rango de un terminal entre redes IPv6 [ref. Rfc3775].

[0030] El protocolo relevante permite a un nodo móvil 10 tanto acceder a la red desde diferentes posiciones, preservando una identidad única, como cambiar dinámicamente el punto de unión manteniendo las conexiones activas existentes.

40 **[0031]** Tal como ya se ha indicado, el protocolo gestiona la movilidad del nodo móvil introduciendo:

- dos direcciones IPv6 diferentes para cada nodo móvil, es decir, una dirección local y una dirección de atención, y

- un agente, llamado Agente local (HA).

[0032] De las dos direcciones diferentes:

45 i) la primera, a saber, la Dirección local (HoA), es una dirección asignada por el proveedor con la que el usuario se ha suscrito al servicio; esta dirección no cambia nunca (al menos para la duración de la sesión entera de trabajo) y se utiliza para identificar unívocamente la identidad del nodo móvil;

ii) la segunda, a saber, la dirección de atención (CoA), es una dirección que pertenece a la red visitada, obtenida de

forma dinámica mediante el nodo móvil a través de configuración automática IPv6 [ref. rfc2462]. Esta dirección localiza la posición actual del nodo móvil y, por tal motivo, cambia en cada movimiento del propio nodo móvil.

5 **[0033]** El agente local reside en la red del proveedor con el que el usuario ha suscrito el servicio (la denominada "red local") y su tarea es redirigir el tráfico destinado al nodo móvil 10 (es decir, el tráfico dirigido a la Dirección local) a la posición actual del propio nodo móvil (es decir, la dirección de atención o CoA).

[0034] Aunque IPv6 Móvil también introduce un modo de comunicación, llamado optimización de ruta, que prevé la comunicación directa entre el nodo móvil 10 y el nodo correspondiente 15, sin que el tráfico pase a través del Agente local 50, la posición del agente local 50 es particularmente importante para el correcto funcionamiento del protocolo y los rendimientos experimentados por el nodo móvil.

10 **[0035]** De hecho, el Tiempo de ida y vuelta (RTT) entre el nodo móvil 10 y el Agente local 50 y, por tanto, su distancia, afectan en gran medida a la latencia de transferencia, es decir, el intervalo de tiempo durante el cual, a raíz de una transferencia, el nodo móvil no es capaz de recibir y enviar los paquetes.

15 **[0036]** Además, si la comunicación entre el nodo móvil 10 y el nodo correspondiente 15 se produce en el modo de túnel bidireccional (por ejemplo, si el nodo correspondiente 15 no soporta las extensiones proporcionadas por Ipv6 Móvil), todo el tráfico de datos debe pasar a través del Agente local 50 y, por lo tanto, la posición de éste último que depende de la posición del nodo móvil 10 afecta en gran medida al retraso de transferencia a la que está sometido el tráfico de datos.

20 **[0037]** La disposición aquí descrita permite asignar al terminal móvil, en el momento de su encendido, un Agente local que es capaz de proporcionar un rendimiento óptimo, es decir, un agente local que está lo más cerca posible, en términos del número de saltos IP, al punto de conexión del terminal móvil. Esto se puede obtener mediante el uso de algunas de las disposiciones disponibles en la literatura para configurar dinámicamente los terminales IPv6 Móvil en su entrada en la red, tal como por ejemplo la disposición descrita en [ref. draft-giaretta-mip6-authorization-eap-00].

25 **[0038]** Cuando, debido a sus continuos movimientos, el nodo móvil se aleja mucho de su propio Agente local (Agente local de servicio) y experimenta un deterioro en el rendimiento del protocolo Ipv6 Móvil, la disposición aquí descrita permite asignar el nodo móvil de un nuevo Agente local (Agente local designado) que es capaz de proporcionar un mejor rendimiento que el anterior (Agente local de servicio).

30 **[0039]** Todo sin causar ninguna interrupción de las aplicaciones en curso y dentro de un procedimiento realizado bajo el control del proveedor con el que el usuario ha suscrito al servicio (proveedor local), que debe autorizar el cambio de Agente local.

[0040] La Figura 4 muestra el escenario general y los elementos de la arquitectura en los que depende la disposición propuesta.

[0041] En particular, se señalan los siguientes:

35 - un servidor de autenticación, autorización y contabilidad 110 del proveedor local del nodo móvil (es decir, el servidor AAA del proveedor con el que el usuario ha suscrito el servicio). En el servidor 110, que corresponde substancialmente a la plataforma indicada con 90 en la figura 3, hay un módulo cuya función es autorizar, controlar y monitorizar el procedimiento de reasignación del Agente local, enviar comandos de configuración e información al nodo móvil 10 y los Agentes locales 70 que están presentes en la red;

40 - un Agente local de servicio 120, es decir, el Agente local que sirve al nodo móvil 10. En el Agente local 120 hay un módulo que interactúa con el servidor de autenticación, autorización y contabilidad 110 y actúa como intermediario en las comunicaciones con el nodo móvil 10;

45 - un Agente local designado 130, es decir, el Agente local designado para servir al nodo móvil 10. En el Agente local 130 se encuentra un módulo que es capaz de recibir desde el módulo de autenticación, autorización y contabilidad 110, la información de configuración para el uso del servicio IPv6 Móvil por los usuarios autorizados (por ejemplo, dirección local, material criptográfico, privilegios concedidos);

- un nodo móvil 10, a saber, el nodo móvil en el que reside un módulo que interactúa con el servidor de autenticación, autorización y contabilidad 110 a través del Agente local de servicio 120 y asegura la supervivencia de sesiones de la aplicación durante el procedimiento de reasignación del Agente local.

50 **[0042]** El mecanismo mediante el cual se gestiona la migración desde el Agente local de servicio 120 al Agente local designado 130 se basa en el enfoque técnico siguiente.

[0043] El nodo móvil 10 declara soportar el cambio de Agente local sin impacto en las comunicaciones actuales (es decir, en una manera "sin costuras") en los mensajes de actualización de enlace que envía a su propio agente

local, usando uno de los bits reservados previstos en [ref. rfc3775, página 39-41]: el Agente local 120 y el servidor 110 son capaces de reconocer qué nodos móviles son capaces de completar el procedimiento.

[0044] El procedimiento puede iniciarse desde el nodo móvil 10, o desde el Agente local de servicio 120, o aún desde el servidor AAA 110 del proveedor local.

5 **[0045]** En los dos primeros casos, el procedimiento es autorizado en cualquier caso por el servidor AAA del proveedor local 110.

[0046] En particular:

10 i) el nodo móvil puede solicitar el inicio de una reasignación del Agente local si detecta la existencia de un Agente local que podría garantizar un mejor rendimiento (por ejemplo, el descubrimiento de un Agente local en su propio enlace a través de la recepción de un mensaje de anuncio de enrutador con el bit H = 1 [ref. 3775, página 61-62]);

ii) el Agente local de servicio 120 puede activar el procedimiento en caso de sobrecarga;

15 iii) el servidor de autenticación, autorización y contabilidad 110 puede dar lugar al procedimiento de reasignación del Agente local con el fin de proporcionar al nodo móvil 10 con un Agente local 130 que permite un mejor rendimiento, usualmente caracterizado por una distancia más corta en términos de saltos IP desde el nodo móvil 10: para hacerlo, el servidor de autenticación, autorización y contabilidad 110 mantiene un registro de todos los Agentes locales presentes en la red, de los cuales los nodos móviles de cada uno de los mismos sirve y de la posición de los propios nodos móviles.

20 **[0047]** La comunicación de los nuevos parámetros de configuración en el nodo móvil 10 (a saber, la dirección del Agente local designado, la nueva dirección local y las asociaciones relacionadas con la seguridad) se obtiene mediante la definición de nuevas opciones de movilidad [ref. rfc3775, página 46-47] dentro de los de mensajes de actualización de enlace (BU) y Reconocimiento de unión (BA): este enfoque tiene la ventaja de liberar al inicio del procedimiento de reasignación del Agente local de eventos de autenticación adicionales. La comunicación con el nodo móvil 10 se puede producir completamente de forma asincrónica (es decir, se puede iniciar en cualquier momento).

25 **[0048]** La supervivencia de sesiones de la aplicación se garantiza mediante la introducción de un mecanismo para la gestión de las direcciones que es similar a la prevista para el procedimiento de “auto-configuración sin estado” de redes IPv6 [ref. rfc2462]: cada Dirección local se asocia a un estado que indica si la dirección se puede utilizar para el inicio de nuevas comunicaciones, o si sólo se puede utilizar para poner fin a las comunicaciones existentes.

30 **[0049]** Independientemente de qué nodo active el procedimiento, se proporciona un mecanismo mediante el cual el nodo móvil 10 comunica a la red 30 si soporta el procedimiento de reasignación del Agente local y, en particular, el cambio de Agente local, sin impacto en las comunicaciones actuales. De hecho, el procedimiento de la disposición propuesta prevé que, durante un período determinado, el nodo móvil 10 utiliza simultáneamente dos Direcciones locales y, a continuación, dos Agentes locales (120 y 130); esto, en particular, implica que el nodo móvil 10 se inicia y mantiene dos asociaciones de seguridad IPsec con dos nodos diferentes.

35 **[0050]** Puede suceder, por lo tanto, que no todos los nodos móviles estén configurados para soportar esta nueva funcionalidad. Además, un terminal (por ejemplo, PDA), puede ser incapaz de soportar el procedimiento, ya que tiene una capacidad de procesamiento limitada o un espacio reducido de memoria.

40 **[0051]** Por esta razón, cada nodo móvil que soporta el procedimiento de reasignación del Agente local comunica esta capacidad del mismo a la red, por ejemplo ajustando a 1 un bit en los mensajes de actualización de enlace (bit R designado con 600 en la figura 13) que lo envía a su propio Agente local; de esta manera, el Agente local de servicio 120 siempre sabe qué nodos móviles son capaces de cambiar el Agente local, sin impacto en las comunicaciones actuales. Esta información, si es necesario, se envía por el Agente local de servicio 120 al servidor de autenticación, autorización y contabilidad 110.

45 **[0052]** Tal como se observó anteriormente, el procedimiento de reasignación del Agente local puede iniciarse mediante el nodo móvil.

[0053] El nodo móvil puede solicitar el inicio del procedimiento cuando recibe un mensaje de anuncio de enrutador (AR) con el bit H ajustado en 1; esto significa, de hecho, que en el enlace donde está, hay un Agente local.

[0054] El servidor de autenticación, autorización y contabilidad puede decidir autorizar, o no autorizar, la solicitud proveniente del nodo móvil 10, dependiendo del estado actual de la red y el perfil del usuario del servicio.

50 **[0055]** En caso de que la solicitud sea autorizada, todo el procedimiento se describe en la figura 5:

- en una etapa 200 el nodo móvil 10 recibe un anuncio de enrutador con el bit H ajustado en 1 y decide iniciar un

procedimiento de reasignación del Agente local;

- en una etapa 202 el nodo móvil 10 envía un mensaje de actualización de enlace (BU) a su propio agente local de servicio 120, en la que se añade una opción de movilidad, llamada opción de movilidad de pistas de reasignación HA. Esta opción es una solicitud de reasignación del Agente local y contiene:

- 5 a) la dirección del Agente local que envió el anuncio de enrutador;
- b) la dirección que el nodo móvil 10 configurado en el enlace visitado y que podría ser la nueva dirección local;

10 - en una etapa 204 el Agente local procesa el mensaje de actualización de enlace tal como se indica en [ref. rfc3775, página 88-92]; en caso de que esté presente una opción de movilidad de pistas de reasignación HA, el Agente local envía al servidor de autenticación, autorización y contabilidad 110 un mensaje de diámetro de la solicitud de reasignación del agente local con los siguientes atributos AVP (Par de valores de atributos):

15 a) Nombre de usuario AVP que contiene el identificador de acceso de red del usuario que solicita la activación del procedimiento. El identificador de acceso de red es el identificador utilizado por el usuario durante la autenticación; en general, es del tipo usuario@dominio. El Agente local de servicio 120 conoce el identificador de acceso de red del nodo móvil que requiere el inicio del procedimiento de reasignación del Agente local, ya que la comparte con el mismo una asociación de seguridad IPsec [ref. draft-giaretta-mip6-authorization-eap-00, página 19];

 b) Dirección local de servicio AVP que contiene la dirección local actualmente asignado al nodo móvil;

20 c) Dirección de agente local designado AVP, y Dirección local designada AVP, respectivamente, que contiene la dirección del Agente local designado y la nueva Dirección local (HoA) propuesta por el nodo móvil en la opción de movilidad de pistas de reasignación HA;

25 - en una etapa 206, el servidor de autenticación, autorización y contabilidad 110 comprueba si el nodo móvil 10 está autorizado para llevar a cabo el procedimiento de reasignación del Agente local; en caso de que la respuesta sea afirmativa, se selecciona un agente local designado 130, posiblemente el señalado por el nodo móvil 10 (las indicaciones proporcionadas por el nodo móvil en la opción de movilidad de pistas de reasignación HA se interpretan como una simple sugerencia, lo que significa que el servidor de autenticación, autorización y contabilidad 110 podría asignar al nodo móvil 10 un Agente local designado y una Dirección local designada diferentes de los requeridos), y se configura dinámicamente en una etapa 208 (por ejemplo, usando el procedimiento descrito en [ref. draft-giaretta-mip6-authorization-eap-00]). Al final de esa comunicación, el Agente local designado 130 tiene asignados los recursos necesarios para gestionar el nodo móvil 10;

30 - cuando la comunicación entre el servidor 110 y el Agente local designado 130 finaliza, en una etapa 210, el servidor 110 envía un mensaje de Diámetro de respuesta de reasignación del Agente local al Agente local de servicio 120 en el que inserta los siguientes atributos AVP:

 a) Nombre de usuario AVP que contiene el identificador de acceso de red del nodo móvil 10;

35 b) Dirección de agente local designado AVP que contiene la dirección del agente local designado 130 asignados al nodo móvil 10;

 c) Dirección local designada AVP que contiene la nueva Dirección local del nodo móvil 10;

40 d) Autorización de por vida AVP que contiene el tiempo de vida, posiblemente igual a infinito, de la anterior Dirección local (Dirección local de servicio). Este valor muestra el tiempo restante durante el cual el nodo móvil 10 puede seguir utilizando el Agente local de servicio, junto con el Agente local designado, para garantizar la supervivencia de sesiones de aplicaciones que ya estaban activas antes de iniciar el procedimiento de redistribución del agente local. En otras palabras, este tiempo de vida muestra en cuánto tiempo debe completarse completamente el procedimiento de reasignación del Agente local;

45 - El Agente local de servicio 120 recibe esta información y en una etapa 212 la comunica al nodo móvil 10, incluyendo la opción de movilidad de datos de reasignación HA en el mensaje de reconocimiento de unión (BA). Esta opción muestra si el procedimiento ha sido exitoso a través del campo Código y contiene la vida útil de la Dirección local anterior, la dirección del Agente local designado y la nueva Dirección local;

50 - el nodo móvil 10 recibe esta información y en una etapa 214 negocia una asociación de seguridad IPsec con el Agente local designado 130. Posteriormente, el nodo móvil 10 puede registrarse a sí mismo con el Agente local designado 130 a través de los mensajes de reconocimiento de unión y actualización de enlace, respectivamente designados por las referencias 216 y 218 en la figura 5. En este período transitorio, el nodo móvil 10 se comunica de manera simultánea usando la dirección local de servicio y la dirección local designada.

[0056] Las comunicaciones entre el servidor de autenticación, autorización y contabilidad y el Agente local designado pueden realizarse de acuerdo a lo que se define en [ref. draft-giaretta-mip6-authorization-eap-00, página 9-12].

5 **[0057]** Tal como se indica en [ref. rfc3775, páginas 18-19], el nodo móvil 10 y el Agente local designado 130 deben compartir una asociación de seguridad IPsec 214 para proteger el tráfico de señalización IPv6 Móvil.

[0058] Como preferencia, a diferencia de lo que se ha descrito en [ref. draft-giaretta-mip6-authorization-eap-00], el servidor de autenticación, autorización y contabilidad 110 no envía al nodo móvil 10 una clave compartida previamente (PSK) para el arranque de dicha asociación de seguridad IPsec a través del IKE (Intercambio de claves de Internet) [ref. Rfc2409].

10 **[0059]** El “secreto” compartido para establecer la Asociación de seguridad puede, de hecho, derivarse del procedimiento de autenticación y, en particular, del material criptográfico exportado mediante el procedimiento EAP (Protocolo de autenticación extensible) utilizado. Esto suponiendo que el nodo móvil utiliza el protocolo EAP [ref. rfc3748] para acceder a la red y que el servidor de autenticación, autorización y contabilidad pueden comunicarse de forma segura la PSK al Agente local designado: un ejemplo de cómo esta comunicación puede realizarse se describe en [ref. draft-giaretta-mip6-authorization-eap-00, página 11-12].

[0060] En el caso de que la solicitud de reasignación del Agente local que procede del nodo móvil 10 no se autorice, todo el procedimiento se describe en la figura 6:

- en una etapa 220 del nodo móvil 10 recibe un anuncio de enrutador con el bit H ajustado en 1 y decide iniciar un procedimiento de reasignación del Agente local;

20 - en una etapa 222 el nodo móvil 10 envía un mensaje de actualización de enlace (BU) a su propio Agente local de servicio 120, en el que se añade una nueva opción de movilidad, denominada opción de movilidad de pistas de reasignación HA;

- en una etapa 224 el Agente local 120 procesa el mensaje de actualización de enlace tal como se indica en [ref. rfc3775, página 88-92];

25 - en una etapa 226 el servidor de autenticación, autorización y contabilidad 110 decide no autorizar la solicitud;

- en una etapa 228 el servidor de autenticación, autorización y contabilidad 110 contesta al mensaje de diámetro de la Solicitud de reasignación del agente local proveniente del agente local de servicio 120 mediante el envío de un mensaje de respuesta de reasignación del Agente local con un Código de Resultado AVP DIAMETER_AUTHORIZATION_REJECTED (autorización de diámetro rechazada) [ref. Rfc3588];

30 - en la etapa 230, a su vez, el agente local de servicio 120 comunica con el nodo móvil 10, el fallo del procedimiento a través de una opción de movilidad de datos de reasignación HA que contiene el valor FALLO en el campo Código.

[0061] El procedimiento de reasignación del agente local se puede solicitar y empezar también por el Agente local de servicio; en particular, el agente local de servicio puede solicitar el inicio del procedimiento para un nodo móvil en caso de que empiece a sobrecargarse y tenga, por consiguiente, dificultades en la gestión de todos los nodos móviles registrados con el mismo.

35

[0062] La figura 7 muestra el flujo del procedimiento en caso de que la solicitud que viene del Agente local de servicio haya sido regularmente autorizada por el servidor de autenticación, autorización y contabilidad. Las etapas que componen el procedimiento son las siguientes:

40 - el Agente local de servicio 120 en una etapa 240 experimenta un disparador que inicia el procedimiento: como se dijo, el caso más significativo es el que tiene una sobrecarga del Agente local;

- el Agente local de servicio 120 activa, en una etapa 242, el procedimiento de reasignación del Agente local mediante el envío al servidor de autenticación, autorización y contabilidad 110 un mensaje de diámetro de solicitud de reasignación del agente local, que contiene el identificador de acceso a la red del nodo móvil que interrumpiría el servicio y la correspondiente Dirección local. El nodo móvil se selecciona entre los que soportan el procedimiento de reasignación del agente local, es decir, entre los que han enviado una actualización de enlace con el bit R igual a 1;

45

- el servidor de autenticación, autorización y contabilidad 110 controla, en una etapa 244, que el agente local de servicio está autorizado para iniciar el procedimiento de reasignación del agente local para el nodo móvil seleccionado. Si la respuesta es afirmativa, el servidor 110 elige, a través de un algoritmo adecuado, un agente local designado 130 para ese nodo móvil;

50 - en una etapa 246 el servidor 110 negocia con el agente local designado 130 el servicio IPv6 Móvil y los correspondientes recursos que se han de asignar. Esto puede realizarse usando, por ejemplo, el procedimiento

descrito en [draft-giaretta-mip6-authorization-eap-00];

- en una etapa 248, una vez completado el procedimiento de asignación de recursos en el agente local designado 130, el servidor 110 envía al Agente local de servicio 120 un mensaje de respuesta de reasignación del agente local en el que se insertan los siguientes atributos AVP:

- 5 a) Nombre de usuario AVP que contiene el identificador de acceso a la red del nodo móvil 10;
- b) Dirección del agente local designado AVP con la dirección del agente local designado;
- c) Dirección local designada AVP con la nueva dirección local;
- d) Autorización de por vida AVP que contiene la vida útil de la dirección local anterior;

10 - tan pronto como el agente local de servicio 120 recibe, en una etapa 250, un mensaje de actualización de enlace por parte del usuario (con el fin de acelerar el procedimiento, el agente local de servicio puede enviar una petición de actualización de enlace, BRR, mensaje solicitando que el nodo móvil 10 envíe de inmediato una nueva actualización de enlace), responde, en una etapa 252, con un mensaje de aceptación del enlace que contiene la opción de movilidad de datos de reasignación HA. Esta opción contiene la vida útil de la anterior dirección local, la dirección local designada y la nueva dirección local (es decir, los datos de configuración proporcionados por el servidor 110 en el mensaje de diámetro anterior de la respuesta de reasignación HA). También en este caso, la PSK para arrancar la asociación de seguridad IPsec entre el nodo móvil y el agente local se deriva del EAP;

- en ese momento, en una etapa 254, el nodo móvil 10 inicia una asociación de seguridad IPsec con el agente local designado y lleva a cabo el registro IPv6 Móvil con el mismo (es decir, la transmisión los mensajes de actualización del enlace y aceptación del enlace, respectivamente, designados mediante las referencias 256 y 258 en la figura 7).

20 **[0063]** También en este caso, el servidor de autenticación, autorización y contabilidad 110 puede decidir no autorizar el procedimiento de reasignación del agente local solicitado por el agente local de servicio; esto se lleva a cabo mediante el envío al agente local de servicio de un mensaje de diámetro de respuesta de reasignación del agente local con el código de resultado AVP igual a DIAMETER_AUTHORIZATION_REJECTED (autorización de diámetro rechazada).

25 **[0064]** La figura 8 muestra el procedimiento de reasignación del agente local en caso de que se inicie mediante el servidor de autenticación, autorización y contabilidad 110.

[0065] Por lo menos dependiendo de las experiencias hasta ahora realizadas por el solicitante, este caso es probablemente el más significativo entre los descritos.

30 **[0066]** El servidor de autenticación, autorización y contabilidad 110 detecta, normalmente durante un procedimiento de re-autenticación, que el nodo móvil está lejos en términos de saltos IP del agente local de servicio y, por tanto, se beneficiará de la asignación de un nuevo agente local. La información sobre la posición del nodo móvil puede obtenerse fácilmente a partir de la dirección IP del servidor de acceso a la red a partir de la que el usuario realizó el procedimiento de re-autenticación.

[0067] El procedimiento comprende las siguientes etapas:

35 - en una etapa 260 el servidor 110 selecciona un agente local designado adecuado, 130, y asigna los recursos, siguiendo, por ejemplo, el procedimiento descrito en [ref. draft-giaretta-mip6-authorization-eap-00];

- una vez que el servidor 110 en una etapa 262 ha configurado el agente local designado 130, se envía en una etapa 264 un mensaje de diámetro de solicitud de activación de la reasignación del agente local al agente local de servicio 120 insertando los siguientes atributos AVP:

- 40 a) Nombre de usuario AVP que contiene el identificador de acceso a la red del usuario;
- b) Dirección local de servicio AVP que contiene la dirección local actualmente asignada al nodo móvil;
- c) Dirección del agente local designado AVP que contiene la dirección del agente local designado;
- d) Dirección local designada AVP que contiene la nueva dirección local asignada al nodo móvil 10;
- e) Autorización de por vida AVP que contiene el tiempo de vida, posiblemente igual a infinito, de la anterior dirección local (Dirección local de servicio);

- en una etapa 266 el agente local de servicio 120 envía inmediatamente un mensaje de nueva solicitud de enlace (BRR) al nodo móvil 10 para solicitar la transmisión de una actualización del enlace. La transmisión de la BRR permite evitar problemas tiempo de espera de comunicación de diámetro entre el agente local de servicio 120 y

el servidor 110, ya que, de lo contrario, no es posible proporcionar de manera determinista cuándo se recibirá la próxima actualización del enlace desde el nodo móvil 10;

5 - después de haber recibido, en una etapa 268, la actualización del enlace del nodo móvil 10 que debe llevar a cabo el procedimiento de reasignación del agente local, en el siguiente reconocimiento del enlace, etapa 270, el agente local de servicio 120 inserta una opción de movilidad de datos de reasignación del agente local que contiene la vida útil de la anterior dirección local, la dirección del agente local designado y la nueva dirección local;

- en una etapa 272 el agente local de servicio 120 responde al servidor 110 con un mensaje de respuesta de activación de la reasignación del agente local, en el que señala que el nodo móvil 10 ha recibido la información para completar el procedimiento;

10 - después, el nodo móvil 10 puede negociar la asociación de seguridad IPsec con el agente local designado 130, etapa 274, y llevar a cabo el registro IPv6 Móvil con el mismo, etapas 276 y 278.

15 **[0068]** Tal como se señaló anteriormente, el nodo móvil se comunica con el agente local de servicio, mediante mensajes de actualización del enlace, si soporta el procedimiento de reasignación del agente local y las opciones de movilidad aquí definidas. Estas informaciones llegan al agente local de servicio y no al servidor de autenticación, autorización y contabilidad; por tal razón, el servidor de autenticación, autorización y contabilidad puede iniciar un procedimiento de reasignación del agente local para un nodo móvil que en la práctica no soporta esa funcionalidad.

20 **[0069]** En tal caso, en una etapa 280 en la figura 9, el agente local de servicio 120 se da cuenta de que el nodo móvil 10 no soporta la funcionalidad solicitada. En una etapa 282 el agente local de servicio 120 se comunica con el servidor 110 que el procedimiento no puede llevarse a cabo a través de un mensaje de respuesta de activación de la reasignación del agente local con el código de resultado AVP igual a DIAMETER_UNABLE_TO_COMPLY (diámetro incapaz de cumplirse).

25 **[0070]** Basado en el procedimiento previamente definido, tras el intercambio con el agente local de servicio de los mensajes de actualización del enlace y de aceptación del enlace que contienen la nueva opción de movilidad y el consiguiente registro con el agente local designado, el nodo móvil tiene dos direcciones locales asociadas a uno o más de los agentes locales.

[0071] La forma en que el nodo móvil gestiona la presencia simultánea de estos dos registros y los criterios basados en los que se elimina por completo el registro del agente local de servicio se describen a continuación.

[0072] En este contexto, es deseable que el procedimiento de reasignación del agente local no tenga influencia en las comunicaciones en curso.

30 **[0073]** Por ejemplo, si el nodo móvil, tan pronto como finaliza el registro con el agente local designado, llevó a cabo la eliminación del registro con el agente local de servicio, posibles sesiones en curso no se mantendrán activas, ya que están identificadas por la dirección local relacionada con el agente local de servicio (es decir, la dirección local de servicio).

35 **[0074]** El enfoque propuesto en la disposición aquí descrita es similar al utilizado en redes IPv6 para configuración de huésped sin estado [ref. 2462].

[0075] La disposición aquí descrita inserta una máquina de estado que regula el uso de una dirección local y, en particular, señala si la dirección local sólo se puede utilizar para las comunicaciones ya activas o también para iniciar nuevas comunicaciones.

[0076] Los estados que se pueden asumir por una dirección local son:

40 - un primer estado, aquí llamado dirección local preferida: es una dirección para la que no hay ninguna restricción de uso de niveles superiores. Esto implica que dicha dirección se puede utilizar para el inicio de nuevas comunicaciones; en el procedimiento aquí descrito, una dirección local está en el estado preferido ya que cuando se le asigna al nodo móvil hasta que se completa el procedimiento de reasignación del agente con la asignación de una nueva dirección local (dirección local designada);

45 - un segundo estado, aquí llamado dirección local obsoleta: es una dirección cuyo uso está permitido sólo para las comunicaciones ya activadas; por lo tanto, no se puede utilizar para el inicio de nuevas comunicaciones. La dirección local pasa de un estado preferido a un estado obsoleto cuando se completa el procedimiento de reasignación del agente local y el propio nodo móvil se ha registrado con el agente local designado; y

50 - un tercer estado, aquí llamado dirección local inválida: una dirección en este estado no se puede utilizar por el nodo móvil para las nuevas comunicaciones, ni para las comunicaciones existentes. La dirección local pasa de un estado obsoleto a un estado inválido cuando el nodo móvil ha terminado todas las comunicaciones previamente activadas con esa dirección; para evitar que una dirección local permanece en el estado obsoleto demasiado tiempo

(por ejemplo, en el caso de comunicaciones con una duración muy larga), una dirección puede pasar al estado inválido también después del transcurso de un tiempo de espera (es decir, la vida señalada mediante el servidor de autenticación, autorización y contabilidad en la autorización de por vida AVP). Cabe señalar que, en la expiración de dicho tiempo de espera, que de todos modos debe caracterizarse por un valor bastante alto, las posibles comunicaciones enlazadas a dicha dirección se detienen.

5

[0077] Para garantizar el correcto funcionamiento del procedimiento, es importante que el servidor de autenticación, autorización y contabilidad 110 llegue a conocer cuándo se ha completado el propio procedimiento; en particular, es necesario prever que el servidor de autenticación, autorización y contabilidad 110 sea informado acerca de cuándo el nodo móvil se registra con el agente local designado y cuándo se elimina su registro con el agente local de servicio. Esta información se pondrá a disposición del servidor de autenticación, autorización y contabilidad 110 por dos razones:

10

- se utilizan como confirmación de la operación correcta del procedimiento, de tal manera que el servidor de autenticación, autorización y contabilidad 110 siempre sabe el agente local que sirve un nodo móvil particular;

15

- se pueden utilizar mediante el servidor de autenticación, autorización y contabilidad 110 para decidir si autoriza un nuevo procedimiento de reasignación del agente local; por ejemplo, el servidor de autenticación, autorización y contabilidad 110 puede decidir no autorizar un nodo móvil o la solicitud del agente local en caso de que el propio nodo móvil no haya completado todavía una reasignación del agente local.

20

[0078] La disposición propuesta prevé que esta información se suministre al servidor de autenticación, autorización y contabilidad 110 usando los mensajes de contabilidad del diámetro; el procedimiento consiste en las etapas utilizadas en la figura 10:

- en una etapa 300 el nodo móvil 10 envía un mensaje de actualización del enlace al agente local designado 130;

- en una etapa 302 el agente local designado 130 responde al nodo móvil 10 con una aceptación del enlace;

25

- después de que el nodo móvil 10 se haya registrado con el agente local designado 130, en una etapa 304 el propio agente local designado 130 envía al servidor 110 un mensaje de inicio de la contabilidad para confirmar el registro realizado; a partir de este mensaje, el servidor 110 comprende que el nodo móvil 10 ha comenzado el procedimiento de reasignación de agente local real y que el nodo móvil está registrado con dos diferentes agentes locales (es decir, el agente local de servicio y el agente local designado);

- en el periodo indicado con 306, sucede que el nodo móvil 10 al mismo tiempo utiliza el agente local de servicio 120 y el agente local designado 130;

30

- en una etapa 308, el nodo móvil 10 envía al agente local de servicio 120 un mensaje de actualización del enlace con un tiempo de vida igual a cero, con el fin de eliminar explícitamente su propio registro, y en una etapa 310 recibe el mensaje de acuse de aceptación del enlace correspondiente. Alternativamente, el nodo móvil 10 puede dejar su propio registro con el agente local de servicio 120 que transcurra de forma espontánea, dejando que se confirme periódicamente su validez mediante el envío de mensajes de actualización del enlace con el agente local de servicio 120;

35

- después de haber eliminado el estado relacionado con el nodo móvil 10, en una etapa 312, el agente local de servicio 120 envía a un servidor de autenticación, autorización y contabilidad 110 un mensaje de diámetro de parada de la contabilidad, tal como ocurre para cualquier servidor de acceso a la red. El servidor 110 comprende a partir de este mensaje que el nodo móvil ya no está registrado en el agente local de servicio 120 y que, por tanto, el procedimiento de reasignación del agente local terminó por completo.

40

[0079] Tal como se indica en [ref. rfc3775, páginas 18-19], es necesario que el nodo móvil y el agente local establezcan una asociación de seguridad IPsec, por ejemplo mediante el uso de intercambio de claves de Internet [ref. rfc2409], antes de intercambiar cualquier mensaje de actualización del enlace o de aceptación del enlace.

45

[0080] A diferencia de lo que se describe en [ref. draft-giaretta-mip6-authorization-eap-00], en la disposición aquí propuesta se establece que la clave compartida previa necesaria para arrancar el intercambio de claves de Internet no se envíe explícitamente al nodo móvil, sino que se derive desde el propio nodo móvil basado en la jerarquía de clave del EAP.

[0081] El procedimiento para derivar y usar esas claves se describe aquí a continuación.

50

[0082] Al final de la comunicación del EAP, el nodo móvil 10 y el servidor de autenticación, autorización y contabilidad 110 comparten dos claves derivadas del procedimiento de autenticación concreto que se utilice: se trata de la clave de sesión maestra (MSK) y clave de sesión maestra extendida (EMSK) [ref. draft-ietf-eap-keying-03, página 13-17]. Esta última clave a su vez puede utilizarse para obtener otras claves, definida como sesión maestra

de aplicación (AMSK), que son directamente utilizadas por las aplicaciones [ref. draft-ietf-eap-keying-03, página 13-17]; en particular, es posible deducir una clave de sesión maestra de aplicación específica para IPv6 Móvil que puede ser utilizado como PSK en fase 1 de IKE.

5 **[0083]** Esta clave se deriva de la EMSK tanto por el nodo móvil 10 como por el servidor de autenticación, autorización y contabilidad 110; éste último posteriormente deberá comunicarlo al agente local. Esta comunicación puede realizarse a través del protocolo de diámetro, por ejemplo, con el enfoque definido en [ref. draft-giaretta-mip6-authorization-eap-00].

[0084] Una función posible para derivar a partir de la EMSK un AMSK para IPv6 Móvil es la siguiente:

- 10 - KDF (K,L,D,O) = T1 | T2 | T3 | T4 | ...
 - T1 = prf (K, S | 0x01)
 - T2 = prf (K, T1 | S | 0x02)
 - T3 = prf (K, T2 | S | 0x03)

donde

- 15 - prf = HMAC - SHA1
 - K = EMSK
 - L = etiqueta clave = "claveMIPv6"
 - D = datos de la aplicación = Dirección agente local
 - O = longitud de salida (2 bytes)
- 20 - S = L | "\ 0" | D | O

[0085] Aquí a continuación se describe un procedimiento que puede usarse mediante el servidor de autenticación, autorización y contabilidad 110 para elegir el agente local designado 130 a asignar al nodo móvil durante el procedimiento de reasignación del agente local.

25 **[0086]** El enfoque se basa en la división de la red acceso del operador en diferentes zonas, cada una caracterizada por la presencia de uno o más agentes locales, tal como se muestra en la figura 11.

[0087] El nodo móvil 10 que se puede encontrar en la zona 400 está normalmente gestionado por el agente local 410 correspondiente a esta zona; después de un movimiento que implica un cambio de zona, 420 ó 440, la red debe decidir si las zonas afectadas están lo suficientemente lejos para justificar el inicio de un procedimiento de reasignación del agente local.

30 **[0088]** Además de las zonas en que se divide la red de acceso, puede ser útil definir una o más zonas de itinerancia 460 que comprenden los agentes locales 470 dedicados a la gestión de los usuarios que están en itinerancia en las redes de otros proveedores 480. La figura 11 muestra estos agentes locales 470 colocados dentro de la red troncal 490 junto a los puntos de interconexión con otras redes.

35 **[0089]** Para gestionar los procedimientos de reasignación del agente local a través de este enfoque, el servidor 110, posiblemente refiriéndose a una base de datos centralizada 500 (por ejemplo, una base de datos LDAP), preferiblemente mantiene las estructuras de datos siguientes:

- Tabla de zonas: en esta tabla, el servidor de autenticación, autorización y contabilidad 110 mantiene la lista de zonas en que se ha dividido la red de acceso y las posibles zonas de itinerancia;
 - Tabla de servidor de acceso a la red: en esta tabla, el servidor de autenticación, autorización y contabilidad 110
- 40 mantiene el identificador de cada servidor de acceso a la red 510 que está presente en la red (por ejemplo, enrutador, punto de acceso) y una lista de información vinculada al mismo, entre los cuales, en particular, la dirección IP y la zona a la que pertenece;
- Tabla del agente local: para cada agente local se mantiene un identificador (por ejemplo dirección IP, identificador de acceso a la red), junto con otra información tanto sobre las características del nodo (tipo, capacidad máxima, etc.)
- 45 como sobre el nivel de carga del nodo actual (es decir, el número de usuarios servidos, que se puede actualizar en función de la información contable). Además, en esta tabla el servidor de autenticación, autorización y contabilidad

110 mantiene la información sobre la zona servida por cada agente local.

5 **[0090]** A partir de la información contenida en estas estructuras de datos, el servidor de autenticación, autorización y contabilidad 110 es capaz de conocer a tiempo en qué zona se puede encontrar un nodo móvil en particular, la zona a la que su agente local de servicio pertenece y la situación de la red mundial. Sin embargo, esta información puede no ser suficiente para decidir cuándo es conveniente, o incluso necesario, realizar el procedimiento de reasignación del agente local; para tal fin, se determina una métrica que permite proporcionar una indicación de la distancia entre zonas y dependiendo de estos parámetros decidir si se debe iniciar el procedimiento.

10 **[0091]** Un ejemplo de métrica estática para la red de la figura 11 y su uso para el fin de tomar una decisión final sobre la ejecución del procedimiento que se muestra en la figura 12. Las filas de la tabla representan zonas posibles (400, 420, 440, 460) que pertenecen al agente local principal, mientras que las columnas representan de manera similar las zonas en las que se puede encontrar el nodo móvil durante sus movimientos. Cada caja contiene un valor que representa la distancia que separa la zona de filas asociadas de la zona de la columna asociada. Al referirse a esta tabla, el servidor de autenticación, autorización y contabilidad 110 puede obtener en cualquier momento la métrica asociada a la distancia desde la zona relacionada con el agente local de servicio a la zona en la que se puede encontrar el nodo móvil. Dependiendo del valor de estos parámetros, el servidor 110 puede decidir si iniciar o no el procedimiento de reasignación del agente local. A modo de ejemplo, es posible asumir una métrica en tres niveles (1, 2 y 3) que tiene el siguiente significado:

20 - 1 = el procedimiento de reasignación del agente local no es necesario (es decir, la zona perteneciente al agente local de servicio coincide con la zona en la que se puede encontrar el nodo móvil, o al menos las dos zonas están muy cerca en términos de número de saltos IP);

- 2 = el procedimiento de reasignación del agente local es opcional (es decir, la zona perteneciente al agente local de servicio no coincide con la zona en la que se puede encontrar el nodo móvil, pero de todos modos las dos zonas no están separadas lo suficiente para que sea estrictamente necesario utilizar el procedimiento de reasignación del agente local);

25 - 3 = el procedimiento de reasignación del agente local es obligatorio (es decir, la zona perteneciente al agente local de servicio está muy lejos de la zona en la que se puede encontrar el nodo móvil de manera que el uso del procedimiento de reasignación del agente local es muy recomendable).

30 **[0092]** Una disposición alternativa prevé la actualización dinámica de la métrica en función de la carga instantánea de la red, que se puede evaluar a través de la estimación del tiempo de ida y vuelta (RTT) entre los diferentes agentes locales y el RTT entre los nodos móviles que están presentes en cada zona y los correspondientes agentes locales de servicio.

[0093] Aquí a continuación se incluye el formato de las opciones de movilidad previamente definidas y los atributos AVP (Par de valor de atributo).

35 **[0094]** La figura 13 muestra el formato del mensaje de actualización del enlace, en el que se señala el bit 600, definido por la disposición aquí descrita: el bit 600 (R) se ajusta en 1 mediante el nodo móvil si soporta con el procedimiento de reasignación del agente local.

[0095] La figura 14 muestra el formato de una opción de movilidad genérica, tal como se especifica en [ref. rfc3775, página 46-47]; tal como se puede observar, se trata de un formato del tipo TLV (Tipo, Longitud, Valor) con la presencia del Tipo 610, Longitud 620 y campos de datos 630.

40 **[0096]** La figura 15 muestra la opción de movilidad de datos de reasignación del agente local. Los campos definidos son los siguientes:

- campo 640 (Código): muestra el resultado del procedimiento. Este campo puede tener los valores siguientes:

i) 0 = Éxito

45 ii) 128 = Fallo

- campo 642 (reservado): campo reservado para usos futuros;

- campo 644 (tiempo de vida): este campo indica el valor en unidades de cuatro segundos de la vida útil de la dirección local actualmente asignada al nodo móvil (la dirección local relacionada con el agente local de servicio, a saber, la dirección local de servicio). Este valor también puede ser infinito;

50 - campo 646 (dirección local): contiene la nueva dirección local asignada al usuario (es decir, la dirección designada);

- campo 648 (dirección del agente local): contiene la dirección del agente local designado.

[0097] La figura 16 muestra el formato de la opción de movilidad de pistas de reasignación del agente local.

5 **[0098]** Cabe señalar que muestra los campos de la dirección local 646 y la dirección del agente local 648 ya introducidos para opción de movilidad de datos de reasignación del agente local. Estos campos pueden contener un valor nulo en caso de que el nodo móvil solicite un procedimiento de reasignación del agente local, sin haber recibido ningún anuncio de enrutador con el bit H = 1.

[0099] Los mensajes de diámetro utilizados en la disposición que aquí se propone son los siguientes:

10 - Solicitud de reasignación del agente local. Este mensaje es enviado por el agente local de servicio al servidor de autenticación, autorización y contabilidad para solicitar el inicio del procedimiento de reasignación del agente local; contiene los siguientes atributos AVP:

- Nombre de usuario AVP;
- Dirección local de servicio AVP;
- Dirección local designada AVP (opcional);
- Dirección del agente local designado AVP (opcional).

15 - Respuesta de reasignación del agente local. Este mensaje es enviado por el servidor de autenticación, autorización y contabilidad para al agente local de servicio para comunicar los nuevos parámetros de configuración que tienen que entregarse al nodo móvil como parte del procedimiento de reasignación del agente local; contiene los siguientes atributos AVP:

- Nombre de usuario AVP;
- 20 - Dirección local designada AVP;
- Dirección del agente local designado AVP;
- Autorización de por vida AVP.

25 - Solicitud de activación de la reasignación del agente local. Este mensaje es enviado por el servidor de autenticación, autorización y contabilidad en caso de que se proponga al agente local de servicio un procedimiento de reasignación del agente local para un nodo móvil particular; contiene los siguientes atributos AVP:

- Nombre de usuario AVP;
- Dirección local de servicio AVP;
- Dirección local designada AVP;
- Dirección del agente local designado AVP;

30 - Autorización de por vida AVP.

- Respuesta a la activación de la reasignación del agente local. Este mensaje es enviado por el agente local de servicio comunicar al servidor de autenticación, autorización y contabilidad que el nodo móvil ha sido advertido sobre la necesidad de llevar a cabo el procedimiento de reasignación del agente local; contiene los siguientes atributos AVP:

35 - Nombre de usuario AVP;

- Resultado AVP.

[0100] Los atributos AVP utilizados y/o definido en este documento son los siguientes (la descripción se basa en convenios y tipos de datos especificados en [ref. rfc3588]):

40 - Nombre de usuario AVP (Código AVP 1). Este AVP contiene el nombre de usuario expresado en la forma de un identificador de acceso a la red. El AVP es del tipo UTF8String.

- Dirección local de servicio AVP. El campo de datos AVP de este AVP es del tipo IPAddress y contiene la dirección local relacionada con el agente local de servicio.

- Dirección local designada AVP. El campo de datos AVP de este AVP es del tipo IPAddress y contiene la dirección

local relacionada con el agente local designado.

- Dirección del agente local designado AVP. El campo de datos AVP de este AVP es del tipo IPAddress y contiene la dirección local del agente designado.

5 - Autorización de por vida AVP (Código AVP 291). Este AVP es del tipo Unsigned32; el valor contenido en el campo de datos AVP representa el tiempo de vida en segundos de la autorización para utilizar los servicios para un determinado usuario. En el caso del procedimiento de reasignación del agente local, este valor indica el tiempo restante durante el cual el nodo móvil puede seguir utilizando el agente local de servicio, junto con el agente local designado, para garantizar la supervivencia de sesiones de aplicaciones que ya estaban activas antes del inicio del procedimiento de reasignación del agente local.

10 **[0101]** El procedimiento de reasignación del agente local descrito se ha detallado, teniendo en cuenta un escenario particular, caracterizado de esta manera:

- la autenticación del nodo móvil para autorizar el acceso a la red se realiza a través de un procedimiento EAP (por ejemplo, EAP-SIM, EAP-AKA) que es capaz de exportar claves que pueden ser utilizadas por otras aplicaciones;

15 - los movimientos del nodo móvil entre las diferentes sub-redes IP son gestionados a través del protocolo IPv6 Móvil, que garantiza la supervivencia de sesiones de aplicaciones a través de eventos de movilidad;

- los mensajes de señalización intercambiados entre el nodo móvil y el agente local se encuentran protegidos (es decir, la autenticación, la integridad y la confidencialidad) a través de una asociación de seguridad IPsec;

- la asociación de seguridad IPsec entre el nodo móvil y el agente local se establece dinámicamente a través del protocolo IKE;

20 - la comunicación entre el servidor de autenticación, autorización y contabilidad y los agentes locales presentes en la red (es decir, el agente local de servicio y el agente local designado) se realiza a través del protocolo de diámetro.

[0102] El procedimiento de la disposición descrita, sin embargo, se puede ampliar, por ejemplo y sin limitación alguna, a situaciones en las que:

25 - la autenticación del nodo móvil se realiza a través de procedimientos diferentes al EAP, pero de todos modos capaces de generar (en el nodo móvil y en el servidor de autenticación, autorización y contabilidad) material criptográfico que puede ser utilizado por otras aplicaciones (por ejemplo, IP móvil);

- los movimientos del nodo móvil se gestionan mediante el uso del protocolo IPv4 Móvil [ref. rfc3344], u otros protocolos de gestión de movilidad basados en principios de arquitectura similares;

30 - los mensajes de señalización intercambiados entre el nodo móvil y el agente local están protegidos a través de un mecanismo que es diferente de IPsec (por ejemplo, la disposición descrita en [ref. draft-ietf-mip6-auth-protocol-00]), pero de todos modos sobre la base de la existencia de un secreto compartido (por ejemplo, clave compartida previamente) entre el nodo móvil y el agente local;

35 - la asociación de seguridad IPsec entre el nodo móvil y el agente local (de servicio o designado) se establece dinámicamente a través del protocolo IKEv2 [ref. draft-ietf-ipsec-ikev2-15], u otros mecanismos que permitan realizar el arranque de una asociación de seguridad IPsec a partir de un secreto compartido (por ejemplo, clave compartida previamente);

- la comunicación entre el servidor de autenticación, autorización y contabilidad y el agente local (agente local de servicio y agente local designado) se realiza utilizando cualquier otro protocolo que es capaz de gestionar el transporte de contenidos de información genérica (RADIUS, SNMP, etc.).

40 **[0103]** En consecuencia, sin apartarse del principio inventivo, las partes constructivas y las realizaciones pueden cambiar, incluso en gran medida, respecto a lo que se describe y se muestra, meramente como un ejemplo no limitativo de posibles realizaciones de la invención, sin por ello apartarse del alcance de la invención, tal como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

- 5 1. Terminal móvil para proporcionar servicios de comunicaciones a al menos un terminal móvil (10) en una red de comunicaciones (30) que comprende una pluralidad de agentes locales (70) y una plataforma de autenticación, autorización y contabilidad, AAA, (90), en el que dicho al menos un terminal móvil (10) comprende medios adaptados para utilizar al menos una dirección para ser servida por un agente local (70) identificado dentro de dicha pluralidad y **caracterizado por el hecho de que** dicha plataforma AAA (90) está configurada para seleccionar, mientras dicho al menos un terminal móvil (10) es servido por un primer agente local (120) en dicha pluralidad, un segundo agente local (130) adaptado para servir a dicho al menos un terminal móvil,
- 10 en el que dicho terminal móvil (10) comprende medios adaptados para recibir de dicha plataforma de autenticación, autorización y contabilidad, AAA, (90), a través de dicho primer agente local (120), información de configuración que está adaptada para configurar el acceso a dichos servicios de comunicación a través de dicho segundo agente local (130), reasignando de este modo el suministro de dichos servicios desde dicho primer agente local (120) a dicho segundo agente local (130).
- 15 2. Terminal móvil según la reivindicación 1, **caracterizado por el hecho de que** dicha información de configuración enviada a dicho al menos un terminal móvil (10) a través de dicho primer agente local (120) comprende parámetros elegidos en el grupo compuesto por:
- la dirección de dicho segundo agente local (130),
 - una nueva dirección asignada a dicho al menos un terminal móvil (10) para las comunicaciones con el segundo agente local (130), y
- 20 - el tiempo de vida de la dirección utilizada por dicho al menos un terminal móvil (10) para las comunicaciones con dicho primer agente local (120).
- 25 3. Plataforma de autenticación, autorización y contabilidad, AAA (90) para su utilización en una red de comunicaciones (30) que comprende al menos un terminal móvil (10) y una pluralidad de agentes locales (70), para proporcionar servicios de comunicación a dicho al menos un terminal móvil (10), en la que dicho al menos un terminal móvil (10) utiliza al menos una dirección destinada a ser servida por un agente local (70) identificado dentro de dicha pluralidad, **caracterizada por el hecho de que** dicha plataforma AAA (90) está configurada para:
- seleccionar, mientras dicho al menos un terminal móvil (10) es servido por un primer agente local (120) en dicha pluralidad, un segundo agente local (130) adaptado para servir a dicho al menos un terminal móvil, y
- 30 - reasignar el suministro de dichos servicios a dicho al menos un terminal móvil (10) desde dicho primer agente local (120) a dicho segundo agente local (130) enviando a dicho al menos un terminal móvil (10) a través de dicho primer agente local (120) información de configuración que está adaptada para configurar dicho al menos un terminal móvil (10) para acceder a dichos servicios a través de dicho segundo agente local (130).
- 35 4. Plataforma de autenticación, autorización y contabilidad, AAA según la reivindicación 3, **caracterizada por el hecho de que** dicha plataforma AAA (90) está configurada para enviar a dicho segundo agente local (130) información de configuración que está adaptada para configurar dicho segundo agente local (130) para permitir el suministro de dichos servicios a dicho al menos un terminal móvil (10).
- 40 5. Plataforma de autenticación, autorización y contabilidad, AAA según la reivindicación 3, **caracterizada por el hecho de que** comprende un primer agente local (120) y un segundo agente local (130) de dicha pluralidad (70), pudiendo ser reasignado el suministro de dichos servicios de comunicaciones a dicho al menos un terminal móvil (10) desde dicho primer (120) a dicho segundo (130) agente local, estando adaptada la reasignación para ser iniciada por dicha plataforma AAA (90).
- 45 6. Plataforma de autenticación, autorización y contabilidad, AAA según la reivindicación 3, **caracterizada por el hecho de que** comprende un primer agente local (120) y un segundo agente local (130) de dicha pluralidad (70), pudiendo reasignar el suministro de dichos servicios de comunicaciones a dicho al menos un terminal móvil (10) desde dicho primer (120) a dicho segundo (130) agente local tras satisfacerse la condición de que dicha plataforma AAA (90) detecta que dicho segundo (130) agente local está adaptado para proporcionar a dicho al menos un terminal móvil (10) dichos servicios de comunicaciones con mejores prestaciones con respecto a dicho primer agente local (120).
- 50 7. Plataforma de autenticación, autorización y contabilidad, AAA según la reivindicación 4, **caracterizada por el hecho de que** dicha información de configuración enviada a dicho segundo agente local (130) comprende parámetros elegidos en el grupo compuesto por:
- un identificador de dicho por lo menos un terminal móvil (10),

- una nueva dirección asignada a dicho al menos un terminal móvil (10) para las comunicaciones con el segundo agente local (130), y

- los parámetros necesarios para la activación de una asociación de seguridad que se pueden utilizar en las comunicaciones entre dicho al menos un terminal móvil (10) y dicho segundo agente local (130).

5 **8.** Plataforma de autenticación, autorización y contabilidad, AAA según la reivindicación 3, **caracterizada por el hecho de que** dicha información de configuración enviada a dicho al menos un terminal móvil (10) a través de dicho primer agente local (120) comprende parámetros elegidos en el grupo compuesto por:

- la dirección de dicho segundo agente local (130),

10 - una nueva dirección asignada a dicho al menos un terminal móvil (10) para las comunicaciones con dicho segundo agente local (130), y

- el tiempo de vida, posiblemente igual a infinito, de la dirección utilizada por dicho al menos un terminal móvil (10) para las comunicaciones con el primer agente local (120).

15 **9.** Plataforma de autenticación, autorización y contabilidad, AAA según la reivindicación 4, **caracterizada por el hecho de que** dicha plataforma AAA (90) está configurada para el establecimiento de una asociación de seguridad (214) para proteger las comunicaciones entre dicho al menos un terminal móvil (10) y dicho segundo agente local (130), estando dicha plataforma AAA (90) también configurada para enviar a dicho segundo agente local (130) por lo menos uno secreto para establecer dicha asociación de seguridad, y para deducir dicho secreto desde dicho por lo menos un terminal móvil (10) a partir del procedimiento de autenticación realizado con dicha plataforma AAA (90).

Fig. 1

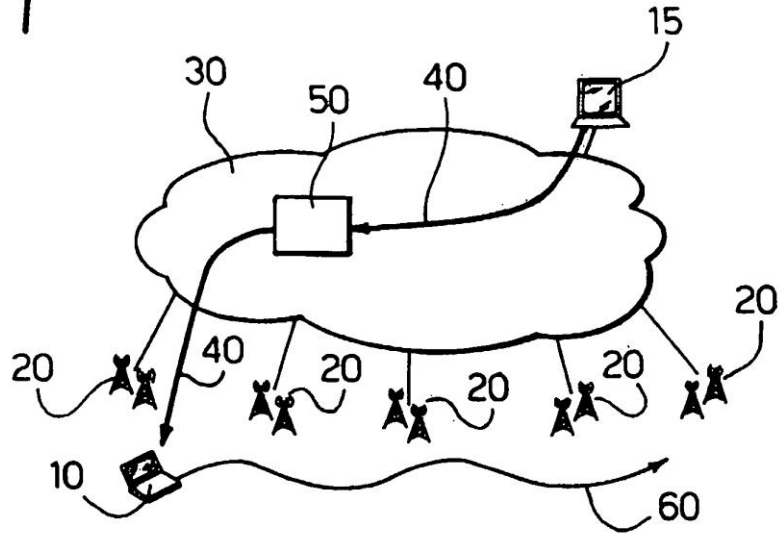


Fig. 2

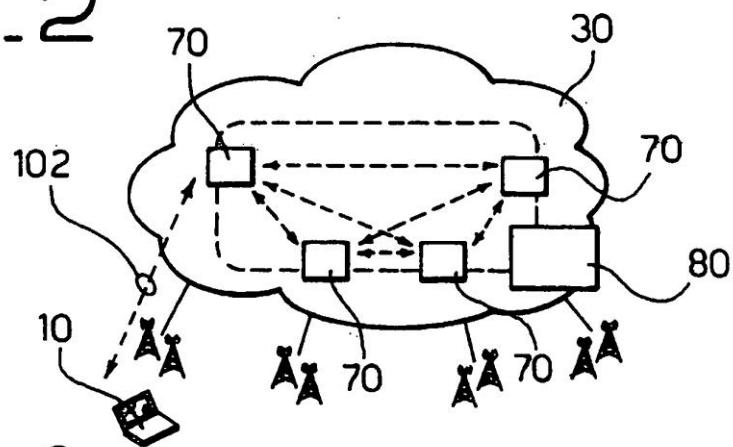


Fig. 3

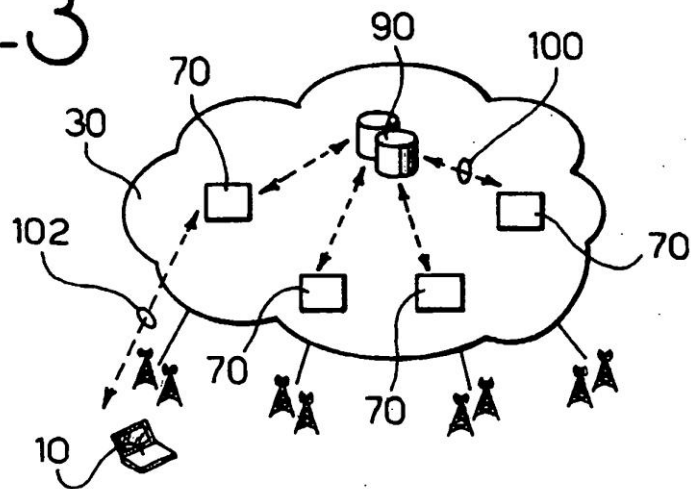


Fig. 4

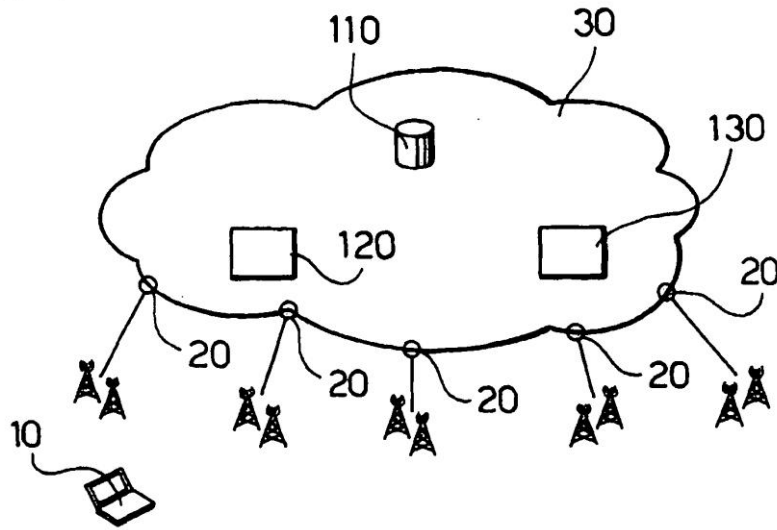


Fig. 5

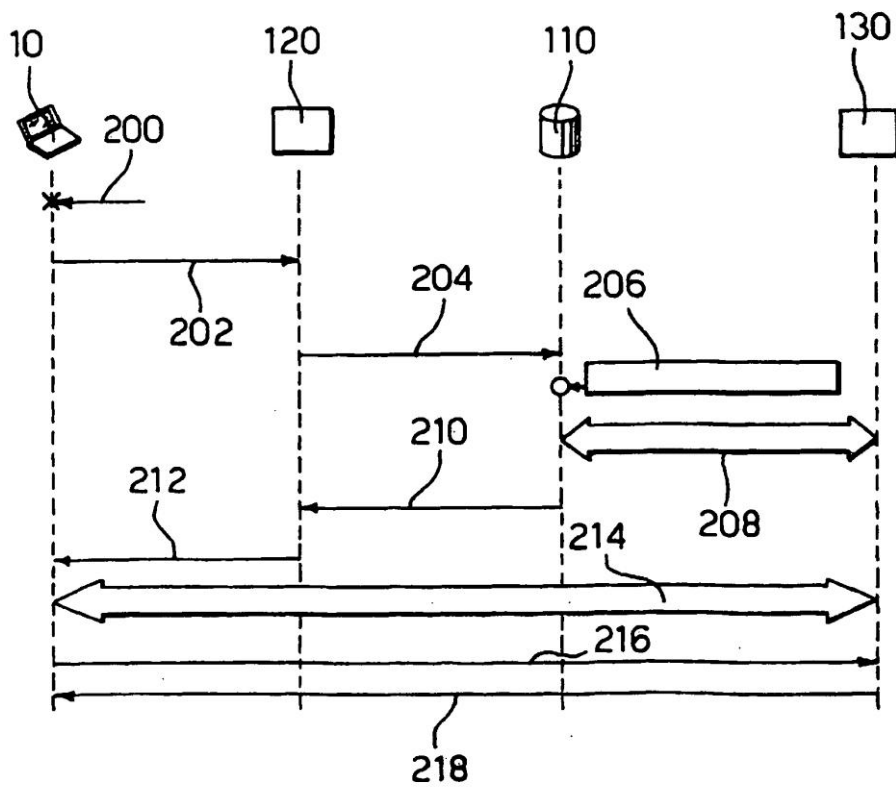


Fig. 6

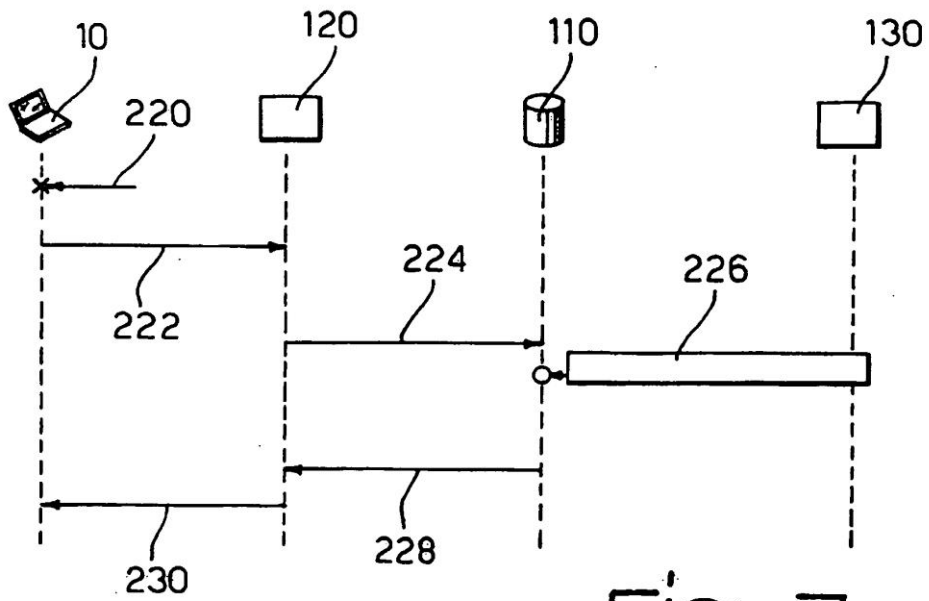


Fig. 7

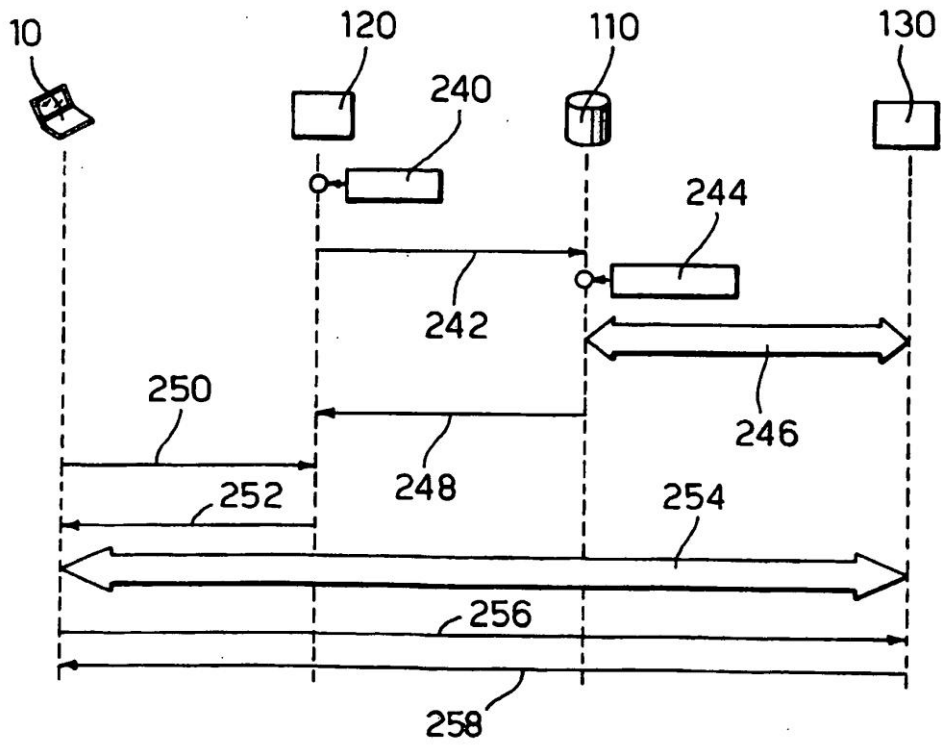


Fig. 8

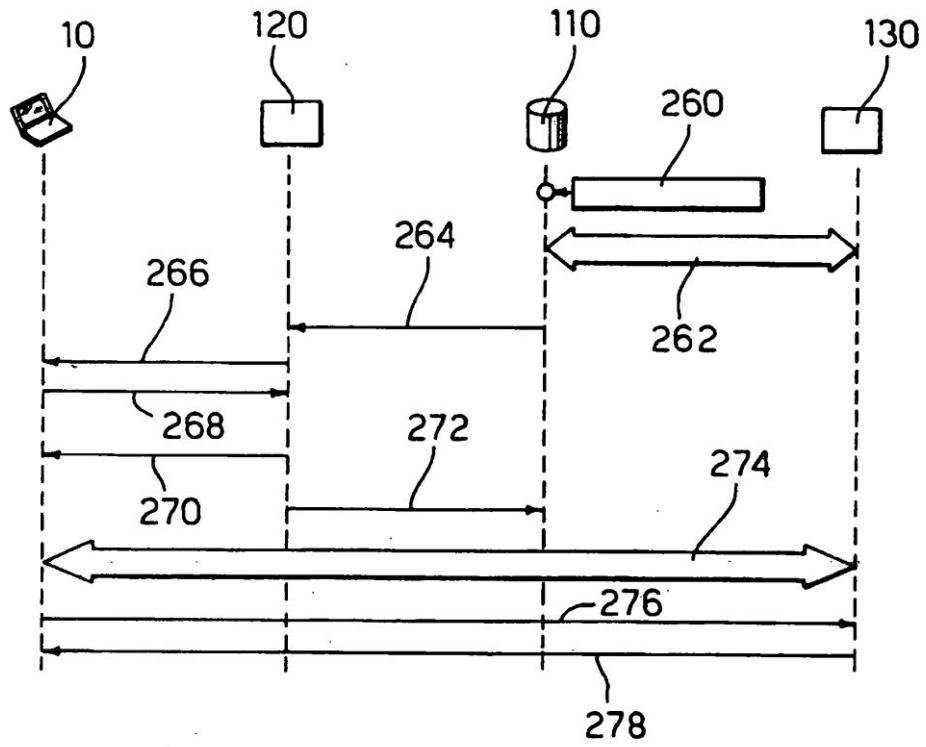


Fig. 9

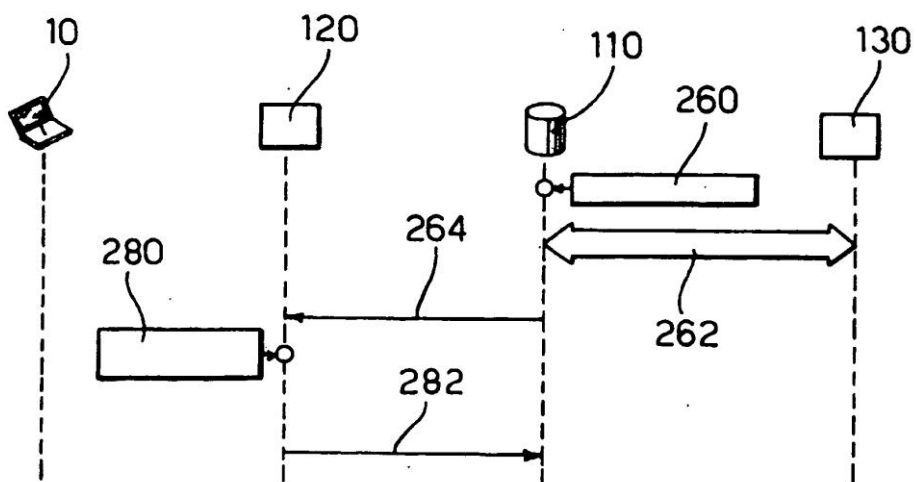


Fig. 10

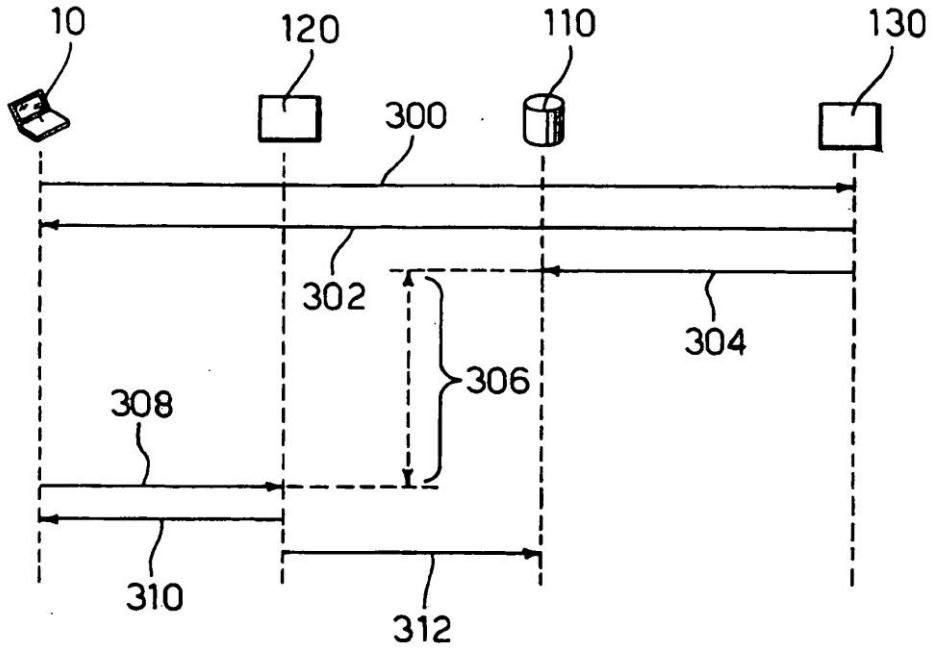


Fig. 11

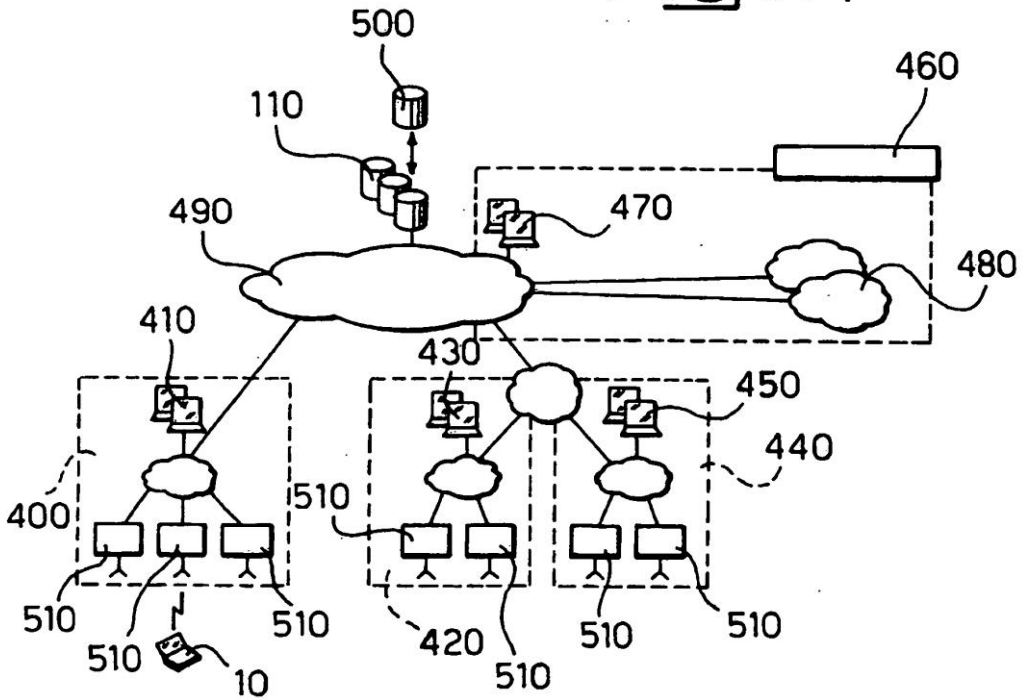


Fig. 12

400	ID Zona	400 (1)	420 (2)	440 (3)	460 Itiner.
420 (1)	1	3	3	3	
440 (2)	3	1	2	3	
440 (3)	3	2	1	3	
460 Itiner.	3	3	3	1	

Fig. 13

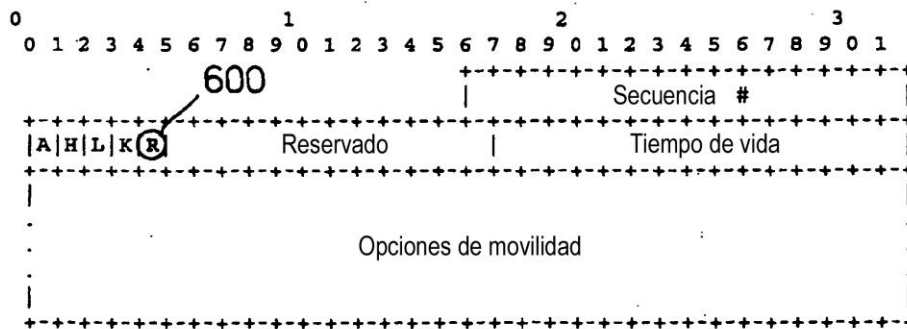


Fig. 14

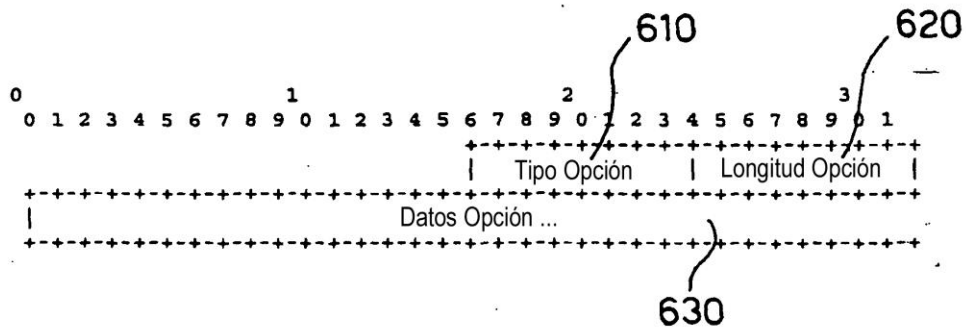


Fig. 15

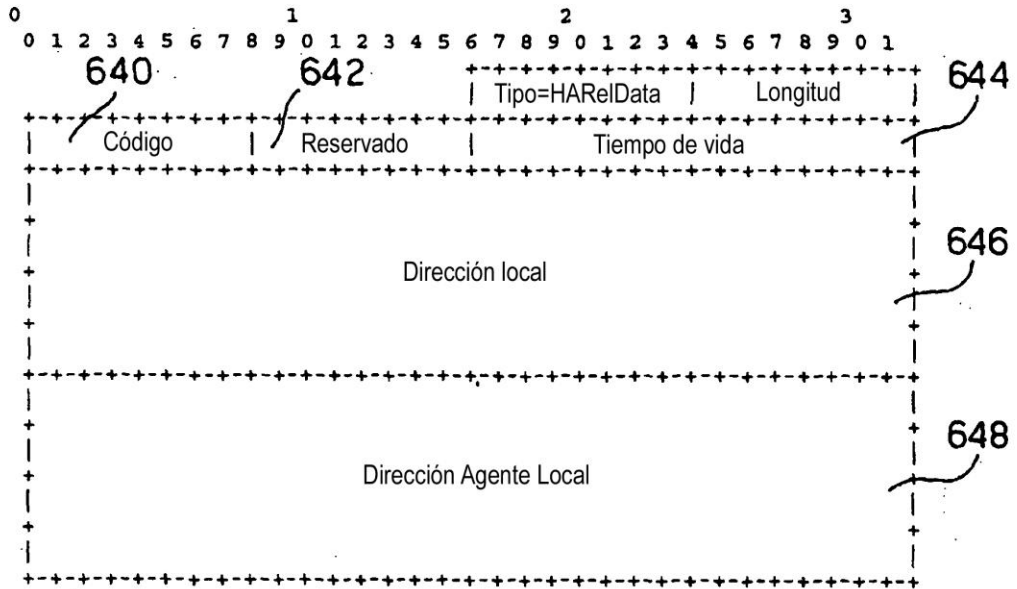


Fig. 16

