(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 409 346**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.06.2005 E 05768210 (6)**

(97) Fecha y número de publicación de la concesión europea: **08.05.2013 EP 1766930**

(54) Título: **Asignación dinámica de agente local y de dirección local en comunicaciones inalámbricas**

(30) Prioridad:

01.07.2004 US 585532 P
02.07.2004 US 585269 P
29.06.2005 US 174261

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2013

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121, US

(72) Inventor/es:

BARANY, PETER ANTHONY;
REZAIIFAR, RAMIN;
BENDER, PAUL E.;
WANG, JUN y
VEEREPALLI, SIVARAMAKRISHNA

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Asignación dinámica de agente local y de dirección local en comunicaciones inalámbricas

La presente Solicitud de Patente reivindica la prioridad respecto a la Solicitud de Patente Provisional No. 60/585,532, con el título "Identificador de Acceso a la Red (NAI) y Procedimiento Asociado" ["Network Access Identifier (NAI) and Method Therefor"], depositada el 1 de julio de 2004, y respecto a la Solicitud de Patente Provisional No. 60/585,269 con el título "MIPv6 Con Dirección Local Dinámica" [MIPv6 With Dynamic Home-Address"], depositada el 2 de julio de 2004, las cuales están transferidas al Cesionario de las mismas.

Antecedentes

Campo

La presente divulgación se refiere, en general, al campo de las comunicaciones inalámbricas y del IP móvil. Más en concreto, las formas de realización divulgadas en la presente memoria están referidas a proporcionar una asignación dinámica de un agente local y una dirección local para un nodo móvil.

Antecedentes

El Protocolo de Internet (IP) Móvil es un protocolo de Internet recomendado diseñado para dar soporte a la movilidad de un usuario. Dicha movilidad resulta importante debido a la proliferación de computadoras portátiles y, por tanto, a la demanda de una conectividad a red continua en cualquier parte en la que resulte encontrarse el usuario.

El avance en las comunicaciones inalámbricas ha provocado, así mismo, la aparición de una diversidad de dispositivos de comunicaciones inalámbricas (por ejemplo, asistentes personales digitales (PDAs), aparatos de bolsillo, teléfonos móviles, etc.) capaces de acceder a Internet y proporcionar servicios de IP, lo que supone una mayor demanda en la infraestructura de Internet actual para proporcionar a los usuarios de aparatos móviles una conectividad sin fisuras y un soporte robusto.

Se reclama la atención sobre el documento de FACCIN MS ET AL: "Aplicación a la IPv6 Móvil Diameter, borrador – le – aaa – diameter movileipv6 – 03.tx" ["Diameter Mobile IPv6 Application, draft - le - aaa - diameter - movileipv6 - 03.tx"] IETF Standard - Working - Draft, INTERNET ENGINEERING TASK FORCE, IETF, CH, 1 de Abril de 2003 (01-04-2003), XP015004098 ISSN: 000-0004.

Así mismo se reclama la atención sobre el documento EP 1075123, el cual describe un sistema dinámico de Agente Local para sistemas de comunicaciones inalámbricas que utiliza la infraestructura existente de las redes de señalización telefónicas y los centros de autenticación celulares mejorados para dar soporte a los Agentes Locales dinámicos, ya sea en redes inalámbricas visitadas o en redes inalámbricas locales de una manera segura para proporcionar servicios de datos por paquetes a una estación de abonado móvil itinerante. Los Centros de Autenticación son desplegados en estas redes como un mecanismo de seguridad celular para proporcionar controles de cualificación de servicio celulares y para impedir el fraude celular mediante el intercambio de claves celulares. El mecanismo de seguridad celular se potencia mediante el uso de una clave adicional, la Clave de IP Móvil Dinámica (DMIPKEY) la cual se utiliza por el Agente Local dinámico en la red inalámbrica visitada para la autenticación de registros de IP Móvil solicitados por la estación de abonado móvil. En los sistema de ANSI la DMIPKEY se puede derivar de la clave de Datos Secretos Compartidos o de la parte A de Datos Secretos Compartidos (SSD_A), dado que esta última se utiliza con fines de autenticación. Con las mejoras necesarias del algoritmo CAVE tanto una estación de abonado móvil equipada con el algoritmo CAVE como su Centro de Autenticación pueden producir de manera independiente la DMIPEKY. Dado que la estación de abonado móvil está equipada con el algoritmo CAVE, la DMIPKEY no necesita ser transmitida por las ondas.

Y, así mismo, se llama la atención sobre el documento US2003176188. Este documento describe una forma para extender la señalización de la Autenticación Autorización y Auditoría del IP Móvil para posibilitar que un nodo solicite de un operador de red combinaciones de capacidades de servicios domésticos y locales (en la indicación de la posición) de una manera eficiente y escalable. Así mismo, permite a los proveedores de servicios locales y foráneos restringir y dar cuenta de los servicios efectivos suministrados en base a una combinación de la política del operador foráneo y local.

Así mismo, se llama la atención sobre el documento de GLASS SUN MICROSYSTEMS T HILLER LUCENT TECHNOLOGIES S JACOBS GT LABORATORIES C PERKINS NOKIA RESEARCH CENTER S: " "Requisitos de Autenticación, Autorización Auditoría del IP Móvil" [Mobile IP Authentication Autorization and Accounting Requierments"] IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, Octubre 2000 (10-2000), XP015008760 ISSN: 0000-0003.

Y finalmente se llama la atención acerca del documento autoría de JOHNSON D: "Soporte de Movilidd en la IPv6" ["Mobility Support in IPv6"] IETF STANDARD - WORKING -DRAFT - INTERNET ENGINEERING TASK FORCE, IETF, CH, 30 de junio de 2003 (30-06-2003) XP015002681 ISSN: 0000-0004.

De acuerdo con la presente invención se proporciona un procedimiento y un aparato para comunicaciones inalámbricas de acuerdo con lo establecido en las reivindicaciones 1 y 6. Formas de realización de la invención se reivindican en las reivindicaciones dependientes.

Breve descripción de los dibujos

La FIG. 1 ilustra un sistema de comunicación configurado para dar soporte al MIPv6;

la FIG. 2 ilustra un sistema de comunicación, en el que pueden ser implementadas las formas de realización divulgadas;

la FIG. 3 ilustra una forma de realización de procedimientos implicados en la asignación dinámica del HA y de la HoA;

la FIG. 4 ilustra un diagrama de flujo de llanadas, el cual puede ser utilizado en una forma de realización para implementar la asignación dinámica del HA y de la HoA;

la FIG. 5 ilustra un diagrama de flujo de llamadas, el cual puede ser utilizado en una forma de realización para implementar la asignación dinámica del HA y de la HoA;

la FIG. 6 ilustra un diagrama de flujo de llamadas, el cual puede ser utilizado en una forma de realización para implementar la asignación dinámica del HA y de la HoA;

la FIG. 7 ilustra un diagrama de flujo de un proceso, el cual puede ser utilizado en una forma de realización para proporcionar una asignación dinámica del HA y de la HoA;

la FIG. 8 ilustra un diagrama de flujo de un proceso, el cual puede ser utilizado en una forma de realización para proporcionar una asignación dinámica del HA y de la HoA;

la FIG. 9 ilustra un diagrama de bloques de un aparato, en el que pueden ser implementadas algunas formas de realización divulgadas; y

la FIG. 10 ilustra un diagrama de bloques de un aparato, en el cual pueden ser implementadas algunas formas de realización divulgadas.

Descripción detallada

Las formas de realización divulgadas en la presente memoria se refieren a la provisión de una asignación dinámica de agente local y de dirección local para un nodo móvil en comunicaciones inalámbricas.

Como referencia y por razones de claridad, diversos acrónimos y abreviaturas utilizadas en la presente memoria se resumen como sigue:

AAA	Autenticación, Autorización y Auditoría
BA	Reconocimiento de Enlace
BU	Actualización de Enlace
CHAP	Protocolo de Autenticación por Negociación de Desafío
CoA	Dirección de Apoyo
DAD	Detección de Direcciones Duplicadas
DHCPv6	Protocolo de Configuración Dinámica de Huesped versión 6
EAP	Protocolo de Autenticación Extensible
HA	Agente Local
HAAA	AAA Locales
HMAC	Código de Autenticación de Mensajes en Hash
HoA	Dirección Local
HoT	Comprobación Local
HoTI	Inic. Comprobación Local

IKE	Intercambio de Clave de Internet
IPsec	Seguridad del Protocolo Internet
IPv6	Versión 6 del Protocolo Internet
IPv6CP	Protocolo de Control IPv6
ISAKMP	Asociación de Seguridad de Internet y Protocolo de Gestión de Claves
LCP	Protocolo de Control de Enlace
MIPv6	Versión 6 del Protocolo Internet Móvil
MN	Nodo Móvil
MS-MPPE	Cifrado Punto a Punto de Microsoft
NAI	Identificador de Acceso a la Red
NAS	Servidor de Acceso a la Red
NCP	Protocolo de Control de Red
PANA	Protocolo para llevar a cabo la Autenticación para el Acceso a la Red
PEAPv2	Versión 2 del Protocolo EAP Protegido
PDSN	Nodo de Servicios de Datos por Paquetes
PPP	Protocolo Punto a Punto
PRF	Función Pseudoaleatoria
RADIUS	Servicio de Usuario de Llamada Entrante de Autenticación Remota
SA	Asociación de Seguridad
SPD	Base de Datos de Plan de Seguridad
TLS	Seguridad de Capa de Transporte
TTLS	TLS Tunelado

Como se utiliza en la presente memoria, un “nodo” puede referirse a un dispositivo implementado para configurar el IP. Un “enlace” puede referirse a una instalación o medio de comunicación a través del cual los nodos pueden comunicar en la capa de enlace. Una “interfaz” puede referirse a una conexión de un nodo a un enlace. Un “prefijo de subred” puede referirse a una cadena de bits que incluye una pluralidad de bits iniciales de una dirección de IP. Un “encaminador” puede incluir un nodo configurado para transferir paquetes de IP no explícitamente dirigidos al mismo. Una “dirección de IP encaminable unidifusión” puede referirse a un identificador que ha establecido una correspondencia con una única interfaz, de tal manera que un paquete enviado a ella desde otra subred de IP es suministrado a la interfaz tal y como se ha establecido la correspondencia.

Un “nodo móvil” (MN) puede referirse a un nodo que puede cambiar su p unto de conexión de un enlace a otro, aunque sigue pudiendo ser alcanzado a través de su dirección local. Un MN puede incluir diversos tipos de dispositivos, incluyendo, (pero no limitado a) un teléfono por cable, un teléfono inalámbrico, un teléfono celular, una computadora portátil, una tarjeta de computadora personal (PC) de comunicación inalámbrica, un asistente personal digital (PDA), un módem externo o interno. En diversas aplicaciones, un MN puede tener diferentes nombres, como por ejemplo unidad de acceso, terminal de acceso, unidad de abonado, estación móvil, dispositivo móvil, unidad móvil, teléfono móvil, móvil, estación remota, terminal remoto, unidad remota, dispositivo de usuario, equipamiento de usuario, dispositivo de bolsillo, etc.

Una “dirección local (HoA)” puede referirse a una dirección de IP encaminable de unidifusión asignada a un MN durante un periodo extenso de tiempo. Un “prefijo de subred local” puede referirse al prefijo de subred de IP correspondiente a una HoA del MN. Una “red local” puede referirse a una red de IP sobre la cual está configurado un prefijo de subred local de MN.

El término “desplazamiento” puede referirse a un cambio en un punto de fijación del MN a Internet de tal manera que ya no está conectado a la misma red como lo estaba con anterioridad. Si un MN no está actualmente fijado a la red local, se dice que el MN está “lejos de casa” (“away from homes”).

Una “dirección de apoyo (CoA)” puede referirse a una unidad de IP encaminable unidifusión asignada a un MN mientras está lejos de casa y en una red visitada (o foránea); el prefijo de subred de la CoA es un prefijo de subred foráneo. Un “prefijo de subred foráneo” puede referirse a cualquier prefijo de subred distinto del prefijo de subred local del MN. Una “red visitada” puede ser cualquier red distinta de la red local del MN.

Un “agente local (HA)” puede referirse a un encaminador (o a una entidad de encaminamiento) con el cual el MN ha registrado su HoA y el actual CoA. Un HA puede estar configurada para interceptar paquetes destinados a la CoA del MN y transferirlos (por ejemplo mediante encapsulación y mediante transmisión por túnel) hacia la CoA registrada del MN. Un “agente local visitador” (HA visitador) divulgado en la presente memoria puede referirse a un HA en una red visitada en la cual está conectado el MN.

Un “nodo correspondiente” (CN) puede incluir un nodo homólogo con el cual esté comunicando un MN. El CN puede ser o bien móvil o bien fijo.

El término “enlace” puede referirse a la asociación de una HoA y una CoA para un MN, junto con el tiempo de vida de esa asociación. Una Actualización de Enlace (BU) puede ser utilizada por un MN para registrar el enlace de su CoA con su HoA. Un Reconocimiento de Enlace (BA) puede ser utilizada para la recepción del reconocimiento de una BU.

Las direcciones de IP hacen posible encaminar paquetes desde un punto terminal de una fuente hasta su destino haciendo posible que los encaminadores transfieran paquetes desde las interfaces de red entrantes hasta las interfaces salientes de acuerdo con las tablas de encaminamiento. Las tablas de encaminamiento típicamente mantienen la información del siguiente salto (interfaz saliente) para cada dirección de IP de destino, la cual acarrea con ella la información que especifica la conexión del punto del nodo de IP (por ejemplo, el prefijo de red). Para mantener las conexiones de capa de transporte existentes cuando un MN se desplaza de un lugar a otro, necesita mantener su misma dirección de IP. Una transferencia correcta de paquetes hasta el punto de conexión actual del MN, sin embargo, depende del prefijo de red contenido en la dirección del IP del MN, la cual cambia en los nuevos puntos de fijación. En otras palabras, para modificar el encaminamiento se requiere una nueva dirección de IP asociada con el nuevo punto de conexión.

El IP Móvil (MIP) ha sido diseñado para resolver este problema haciendo posible que un MN utilice dos direcciones de IP: una HoA estática y una CoA (por ejemplo, véase la versión 6 del MIP (MIPv6) o la versión 4 del MIP (MIPv4), promulgada por la INTERNET ENGINEERING TASK FORCE (IETF) Request for comments (RFC) 3775 o RFC344). La HoA es estática y se utiliza por ejemplo, para identificar una red local del MN y / u otra información de conexión (como por ejemplo conexiones de TCP). La CoA cambia en cada nuevo punto de conexión y puede ser considerada como la dirección topológicamente significativa del MN. La CoA incluye el prefijo de red y, por tanto, identifica el punto de fijación del MN con respecto a la topología de red. La CoA hace parecer que el MN es continuamente capaz de recibir datos en su red local, donde un HA está designado para el MN. Cuando el MN está “lejos de casa” y está conectado a una red visitada, el HA recoge todos los paquetes destinados a la HoA del MN y los dispone para entregarlos en el punto de fijación actual del MN.

Mientras se encuentra “lejos de casa” un MN adquiere una CoA (por ejemplo, a partir de un encaminador o un anuncio de agente) desde una red visitada en conexión con su actual punto de fijación. El MN, a continuación, registra su nueva CoA con su HA llevando a cabo una BU. Para conseguir un paquete hasta el MN desde su red local, el HA transmite el paquete desde la red local hasta la CoA. Esto implica la modificación del paquete de forma que la CoA aparece como la dirección de IP de destino. (Cuando el paquete llega a la CoA, se aplica la transformación inversa, de modo que el paquete parece tener la CoA del MN como la dirección de IP de destino.

Como tal, el MIP hace posible que un MN se desplace sin junturas de una red a otra sin modificar su HoA, y recibe continuamente datos utilizando esta dirección con independencia del punto de fijación actual del MN con Internet. Como resultado de ello, el desplazamiento del MN lejos de su red local es transparente para los protocolos de transporte, los protocolos y aplicaciones de capa alta.

En la MIPv6, la asignación de un HA y de una HoA es estática. Aunque esto está previsto para evitar que un MN utilice su SA del IPsec para llevar a cabo una BU en favor de otro MN con el mismo HA, ello puede provocar algunas consecuencias deseables, de acuerdo con lo descrito más adelante.

A modo de ejemplo, la FIG. 1 ilustra un sistema 100 de comunicación en el que un MN 110 que tiene una HoA , está lejos de una red 120 local y conectado a una red 130 visitada. El MN 110 ha adquirido una CoA en conexión con la red 130 visitada, y registrado el enlace de su HoA y su CoA con un HA 125 en la red 120 local.

En un ejemplo, la red 120 local puede estar situada, por ejemplo, en San Diego, California, mientras que la red 130 visitada puede estar situada, por ejemplo, en Tokio, Japón. (En otros ejemplos, la red 120 local y la red 130 visitada pueden estar en el mismo país pero en diferentes ciudades, u otras configuraciones). El MN 110 puede estar en

comunicación con un CN 140 (por ejemplo, un proveedor local de servicios de Internet o un dispositivo móvil) a través de la red 130 visitada. En este caso, los paquetes procedentes del CN 140 hasta el MN 110 (por ejemplo, ambos en Tokio) tienen que ser en primer lugar encaminados hacia el HA 125 (por ejemplo, en San Diego), el cual, a continuación, transfiere los paquetes (por ejemplo, por vía satélite y / o por cable submarino) hasta el MN 110 a través de su CoA. En otras palabas, cuando el MN 110 está "lejos de casa", el MIP actual proporciona un servicio de acceso remoto a través de su red local, lo que puede provocar que las transmisiones de paquetes sean ineficientes y / o fiables en algunas situaciones, de acuerdo con lo descrito con anterioridad. Sería deseable que el MN 110 recibiera el servicio de acceso local en la red 130 visitada, sin tener que atravesar la red 120 local cada vez.

Formas de realización descritas en la presente memoria se refieren a la provisión de una asignación dinámica del HA y de la HoA para un MN en relación con su actual punto de conexión, de tal manera que se permite que el MN reciba el servicio de acceso local.

La FIG. 2 ilustra un sistema 200 de comunicación, en el cual pueden ser implementadas diversas formas de realización divulgadas. A modo de ejemplo, un MN 210 está lejos de una red 220 local y está conectado a una red 230 visitada. Un HA 235 visitante sobre la red 230 visitada y una HoA son asignados al MN 210. El MN 210 puede, así mismo, adquirir una CoA asociada con la red 230 visitada, y registrar el enlace de su HoA y su CoA con el HA 235 visitante llevando a cabo una BU. De esta manera, el MN 210 se beneficia de la recepción del servicio de acceso local desde la red 230 visitada. Por ejemplo, los paquetes transmitidos entre el MN 210 de un CN 240 pueden ser encaminados a través del HA 235 visitante el cual es "local" (o próximo) tanto al MN 210 como al CN 240, haciendo con ello más eficientes y fiables las transmisiones de paquetes. En algunas formas de realización, el uso o la selección de la red 230 visitada por el MN 210 y el CN 240 se puede basar, por ejemplo, en los emplazamientos del MN 210 y del CN 240, del estado de la carga de la red, o en otras condiciones / criterios, etc.

La FIG. 3 ilustra una forma de realización 300 de procedimientos implicados en la asignación dinámica de un HA y de una HoA para un MN (por ejemplo, en el sistema 200 de comunicación de la FIG. 2). En la etapa 310, un MN accede a una red visitada (lo que puede acarrear, por ejemplo, la configuración del enlace de datos y del protocolo de negociación para una identificación de la red visitada). En la etapa 320, la red visitada lleva a cabo la autenticación con la red local del MN (por ejemplo, un servidor de AAA local en la red local). En la etapa 330, la red visitada asigna un HA visitado y una HoA (o una porción de una HoA) al MN. En la etapa 340, el MN lleva a cabo un enlace seguro con el HA visitante (el cual puede, así mismo, incluir una asociación de seguridad de negociación con el HA visitante). En la etapa 350, el MN continúa con las comunicaciones utilizando el HA y la HoA visitantes. Formas de realización descritas a continuación proporcionan algunos ejemplos.

La FIG. 4 ilustra un diagrama 400 de flujo de llamadas, el cual puede ser utilizado en una forma de realización para implementar la asignación dinámica del HA y de la HoA para un MN (por ejemplo en la forma de realización de la FIG. 3). A modo de ejemplo, el diagrama 400 del flujo de llamadas ilustra las negociaciones que tienen lugar entre un MN 410 y un servidor 420 de acceso a la red (NAS) sobre una red visitada (no explícitamente mostrada), y un servidor 440 de AAA local (no explícitamente mostrado), para asignar el HA 430 visitante sobre una red visitada y una HoA para el MN 410. En una forma de realización, el NAS 420 puede incluir un PSDN, trabajando en combinación con un servidor del DHCP sin estado, como por ejemplo un servidor de la DHCPv6 sin estado (por ejemplo, tal y como se especifica en las RFCs 3315 y 3736 de la IETF). Adviértase que, por razones de sencillez e ilustración, el servidor del DHCP sin estado se muestra como colocado por el NAS 420. En otras formas de realización pueden estar situados de forma separada.

En la etapa 451, el MN 410 configura el enlace de datos, por ejemplo, llevando a cabo el LCP del PPP (tal y como se especifica en la RFC 1661 de la IETF), y negocia el uso de un protocolo de autenticación, como por ejemplo el PAP (por ejemplo, tal y como se especifica en la RFC 1661 de la IETF) o en el CHAP (por ejemplo, tal y como se especifica en la RFC 1994 de la IETF).

En la etapa 452, el MN 410 autentica con el NAS 420 a través de o bien el PAP o el CHAP. El NAS 420 puede autenticar el MN 410 con el servidor 440 la AAA local por medio de un mensaje de solicitud de acceso especificado por el protocolo RADIUS (por ejemplo, tal y como se especifica en las RFCs 2865 y 3162 de la IETF). En otras formas de realización, el protocolo de Diameter (por ejemplo, tal y como se especifica en la RFC 3588 de la IETF) puede, así mismo, ser utilizado.

En la etapa 453, el servidor 440 de AAA local autentica el MN 410 y responde al NAS 420 por medio de un mensaje de acceder - aceptar especificado por el protocolo de RADIUS. El mensaje de acceder - aceptar puede incluir un atributo de vendedor - específico de RECV-KY del MS - MPPE (como por ejemplo se especifica en la RFC 2548 de la IETF), que contenta la clave precompartida del MN 410. La clave precompartida puede ser utilizada durante los IKE / ISAKMP (por ejemplo tal y como se especifica en las RFCs 2408 y 2409 de la IETF) por el MN 410 y el HA 430 visitante (por ejemplo, véase la etapa 459 más adelante). En el caso de que el MN 420 autentique con el CHAP (por ejemplo, como se describe en la etapa 451 anterior), la clave precompartida del MN 410 puede ser calculada como sigue: PRF (MN - HAAA_Shared_Secret, CHAP_Challenge, NAI). La función pseudoaleatoria (PRF) puede ser un HMAC. El NAI puede ser el identificador de acceso a red del MN 410. El "MN-HAA_SHARED_SECRET" puede ser suministrado de antemano tanto en el MN 410 como en el servidor de AAA local.

En la etapa 454, el MN 410 lleva a cabo el IPv6CP del PPP (por ejemplo, tal y como se especifica en la RFC 2472 de la IETF) para negociar un ID de interfaz de 64 bits, cuál MN 410 puede utilizar para configurar su dirección de enlace local de la IPv6 (por ejemplo tal y como se especifica en las RFCs 2460 a 2462 y 3513 de la IETF) y la CoA (por ejemplo tal y como especifica en la RFC 3775 de la IETF) a través de una autoconfiguración de dirección sin estado (por ejemplo, tal y como se especifica en la RFC 2462 de la IETF).

En la etapa 455, el NAS 420 envía un mensaje de Anuncio de Encaminador (por ejemplo, tal y como se especifica en la RFC 2461 de la IETF) al MN 410 que contiene un prefijo /64, de cuál MN 410 puede utilizar para construir su CoA mediante la adición del ID de la interfaz de 64 bits negociada en la etapa 454 al prefijo /64 . En una forma de realización, el mensaje de Anuncio de Encaminador puede incluir “M - flag = 0, O - flag = 1, Router LifeTime, A - flag = 1, L - flag = 0” (por ejemplo, tal y como se especifica en la RFC 2461 de la IETF). La M - flag puede ser fijada a ‘0’, que indique que el MN 410 puede utilizar el servidor de la DHCPv6 sin estado para configurar otros parámetros, incluyendo (pero no limitado a) la dirección del HA 430 visitante y la HoA del MN 410, tal y como se describe con mayor detalle más adelante.

En la etapa 456, el NAS 420 asigna una dirección para el HA 430 visitante y una HoA para el MN 410. El NAS 420 puede almacenar dicha información en el servidor de la DHCPv6 sin estado.

En la etapa 457, el MN 410 utiliza el servidor de la DHCPv6 sin estado para obtener la dirección del HA 430 visitante y la HoA para el MN 410. En algunas formas de realización la dirección del HA 430 visitante y la HoA para el MN 410 pueden ser almacenadas en el servidor de la DHCPv6 sin estado como opciones de información del vendedor específico (por ejemplo, tal y como se especifica en la RFC 3315 de la IETF).

En la etapa 458, el NAS 420 crea una entrada para la SPD (tal y como se especifica en la RFC 2401 de la IETF) en el HA 430 visitante, por ejemplo, para los fines de la BU, la BA, la HoTi , la HoT y otros mensajes (por ejemplo, tal y como se especifica en la RFC 3775 de la IETF). En algunas formas de realización el NAS 420 puede utilizar la interfaz suministrada por el vendedor NAS 430 visitante para llevar a cabo dicha entrada (por ejemplo, tal y como se especifica en la RFC 2750 de la IETF).

En la etapa 459 el MN 410 lleva a cabo la Fase 1 del IKEv1 utilizando un modo agresivo con una clave compartida (por ejemplo, tal y como se especifica en las RFCs 2409 y 2460 de la IETF) con el HA 430 visitante, para negociar la SA del ISAKMP y generar las claves para los mensajes del ISAKMP de la Fase 2 de la IKEv1.

En la etapa 460, el MN 410 lleva a cabo la Fase 2 de la IKEv1 utilizando el modo Rápido (por ejemplo, tal y como se especifica en las RFCs 2409 y 2460 de la IETF) con el HA 430 visitante, para negociar la SA de la IPsec (por ejemplo, tal y como se especifica en la RFC 2401 de la IETF) y generar claves para los mensajes negativos del ISAKMP para asegurar la BU, BA, HoTi , HoT, y otros mensajes (por ejemplo, tal y como se especifica en la RFC 3775 de la IETF).

En la etapa 461, el MN 410 registra el enlace de su HoA y de la CoA con el HA 430 visitante mediante la realización de una BU. Ello puede ser protegido por la IPsec (por ejemplo, véase la etapa 460 anterior).

En la etapa 462, el HA 430 visitante lleva a cabo una DAD apoderada (por ejemplo, tal y como se especifica en las RFCs 2462 y 3775 de la IETF) a favor del MN 410, para asegurar que ningún otro nodo sobre el enlace del HA 430 visitante esté utilizando la HoA del MN 410.

En la etapa 463, el MN 410 recibe una BA del HA 430 visitante en respuesta a su BU en la etapa 461. Ello puede, así mismo, ser protegido por la IPsec (por ejemplo, véase la etapa 460 anterior).

La FIG. 5 ilustra un diagrama 500 de flujo de llamadas, el cual puede ser utilizado en una forma de realización para implementar una asignación dinámica del HA y de una HoA para un MN. Por razones ilustrativas y de claridad, a los mismos elementos se les asignan los mismos numerales en las FIGs. 4 y 5. El diagrama 500 de flujo de llamadas puede, así mismo, compartir algunos de los elementos característicos utilizados en el diagrama 400 del flujo de llamadas de la FIG. 4, tal y como se describe con mayor detalle más adelante.

En la etapa 551, el MN 410 lleva a cabo el LCP del PPP (tal y como se especifica en la RFC 1661 de la IETF) para configurar el enlace de datos y negociar el uso del EAP (por ejemplo, tal y como se especifica en la RFC 3487 de la IETF) para autenticación.

En la etapa 552, el MN 410 autentica con el servidor 440 del AAA local a través de o bien los EAP - TTLS (por ejemplo, tal y como se especifica en el “Protocolo de Autenticación de la TLS Tunelado (EAP - TTLS)”, borrador de la IETF, julio 2004), o bien en la PEAPv2 (por ejemplo, tal y como se especifica en la “Versión 2 del Protocolo EAP Protegido”, borrador de la IETF, octubre 2004). La comunicación del EAP entre el MN 410 y el servidor 440 del AAA Local puede producirse a través del PPP entre el MN 410 y el NAS 420, y a través del protocolo RADIUS (tal y como se especifica en la RFC 2865 de la IETF) entre el NAS 420 y el servidor 440 del AAA local. En otras formas de realización, el protocolo Diameter (tal y como se especifica en la RFC 3588 de la IETF) puede ser utilizado entre el NAS 420 y el servidor 440 del AAA local. Como parte de este procedimiento global el NAS 420 envía un mensaje de acceder -- solicitar (por ejemplo, especificado por el protocolo RADIUS) hasta el servidor 440 del AAA local, para

obtener la clave precompartida del MN 410 (por ejemplo, para ser utilizada en el transcurso de los IKE / ISAKMP por el MN 410 y el HA 430 visitante *infra*) y el material cifrante para el cifrado y la autenticación de datos del MN 410 y el NAS 420 (como parte de la funcionalidad de los EAP - TTLS o de la PEPv2). El servidor 440 del AAA local responde al NAS 420 con un mensaje de acceder - aceptar (por ejemplo especificado por el protocolo RADIUS). El mensaje acceder - aceptar incluye un atributo de vendedor específico de MS - MPPE - Recv - Key (por ejemplo, tal y como se especifica en la RFC 2548 de la IETF), que contiene la clave precompartida del MN 410.

En la etapa 553, el MN 410 lleva a cabo el IPv6CP del PPP (por ejemplo, tal y como se especifica en la RFC 2472 de la IETF) para negociar un ID de interfaz de 64 bits, cuál MN 410 puede utilizar para configurar su dirección de enlace local de la IPv6 (por ejemplo, tal y como se especifica en la RFC 2460 de la IETF) y su CoA (tal y como se especifica en la RFC 3775 de la IETF) por medio de una autoconfiguración sin estado (tal y como se especifica en la RFC 2462 de la IETF).

En la etapa 554 el NAS 420 envía un Anuncio de Encaminador (por ejemplo, tal y como se especifica en la RFC 2461 de la IETF) hasta el MN 410 que contiene un prefijo /64, de cuál MN 410 puede utilizar para construir su CoA mediante la adición del ID de interfaz de 64 bits negociado en la etapa 553 por encima del prefijo /64. En una forma de realización, el anuncio del encaminador puede incluir “M - flag = 0, O - flag = 1, Router Lifetime, A - flag = 1, L - flag = 0” (por ejemplo, tal y como se especifica en la RFC 2461 de la IETF). El M - flag puede establecerse en ‘0’ que indica que el MN 410 puede utilizar una autoconfiguración de dirección sin estado para configurar su CoA. El O - flag puede establecerse en ‘1’, que indica que el MN 410 puede utilizar el servidor de la DHCPv6 sin estado para configurar otros parámetros, incluyendo (pero no limitado a) la dirección del HA 430 visitante y la HoA del MN 410, tal y como se describe con mayor detalle a continuación.

En la etapa 555, el NAS 420 asigna una dirección para el HA 430 visitante y una HoA para el MN 410. El NAS 420 puede almacenar dicha información en el servidor de la DHCPv6 sin estado.

En la etapa 556, el MN 410 utiliza el servidor de la DHCPv6 sin estado para obtener la dirección del HA 430 visitante y su HoA. En algunas formas de realización, la dirección del HA 430 visitante y de la HoA para el MN 410 pueden ser almacenadas en el servidor de la DHCPv6 sin estado como opciones de información del vendedor específico (tal y como se especifica en la RFC 3315 de la IETF).

En la etapa 557, el NAS 420 crea una entrada de la SPD en el HA 430 visitante, por ejemplo, para los fines de las BU, BA, HoTi , HOT y otros mensajes (por ejemplo, tal y como se especifica en la RFC 3775 de la IETF). En algunas formas de realización, el NAS 420 puede utilizar la interfaz suministrada por el vendedor del HA 430 visitante para llevar ello a cabo, (por ejemplo, tal y como se especifica en la RFC 2570 de la IETF).

En la etapa 558, el MN 410 lleva a cabo la Fase 1 de la IKEv1 utilizando un modo agresivo con la clave precompartida (por ejemplo, tal y como se especifica en las RFCs 2409 y 2460 de la IETF), con el HA 430 visitante para negociar la SA del ISAKMP y generar las claves para los mensajes del ISAKMP de la Fase 2 de la IKEv1.

En la etapa 559, el MN 410 lleva a cabo la Fase 2 de la lhEev1 utilizando el modo rápido (por ejemplo, tal y como se especifica en las RECs 2409 y 2460 de la IETF) con el HA 430 visitante, para negociar la SA de la IPsec y generar las claves para los mensajes no de ISAKMP para asegurar las BU, BA, HoTi, HoT, y otros mensajes (por ejemplo, tal y como se especifica en la RFC 3775 de la IETF).

En la etapa 560, el MN 410 registra el enlace de sus HoA y CoA con el HA 430 visitante llevando a cabo una BU. Ello puede ser protegido por la IPsec (por ejemplo, véase la etapa 559 anterior).

En la etapa 561, el HA 430 visitante lleva a cabo una DAD apoderada (por ejemplo, tal y como se especifica en las RFCs 2462 y 3775 de la IETF) a favor del MN 410, para asegurar que ningún otro nodo sobre el enlace del HA 430 visitante esté utilizando la HoA del MN 410.

En la etapa 562, el MN 410 recibe una BA del HA 430 visitante en respuesta a su BU en la etapa 560. Ello puede, así mismo, ser protegido por la IPsec (por ejemplo, véase la etapa 560 anterior).

La FIG. 6 ilustra un diagrama 600 de flujo de llamadas, el cual puede ser utilizado en una forma de realización para implementar una asignación dinámica del HA y de la HoA para un MN. Con fines ilustrativos y de claridad, a los mismos elementos se les asignan los mismos numerales en las FIGs. 4, 5 y 6. El diagrama 600 de flujo de llamadas puede, así mismo, compartir algunos de los elementos característicos utilizados en los diagramas 400 y 500 de flujo de llamadas, tal y como se describen con mayor detenimiento a continuación.

En la etapa 651, el MN 410 lleva a cabo el LCP del PPP (tal y como se especifica en la RFC 1661 de la IETF) para configurar el enlace de datos y negociar el uso de, o bien el PAP (tal y como se especifica en la RFC 1661 de la IETF) o bien el CHAP (tal y como se especifica en la RFC 1994 de la IETF) con fines de autenticación.

En la etapa 652, el MN 410 autentica con el NAS 420 a través de, o bien el PAP o bien el CHAP. El NAS 420 puede autenticar el MN 410 con el servidor 440 del AAA local a través de un mensaje de acceder - solicitar especificado por

el protocolo RADIUS (tal y como se especifica en la RFC 2885 de la IETF), o con el protocolo de Diámetro (tal y como se especifica en la RFC 3588 de la IETF), tal y como se describió con anterioridad.

En la etapa 653, el servidor 440 del AAA local autentica el MN 410 y responde al NAS 420 por medio de un mensaje de acceder - aceptar especificado por el protocolo RADIUS. El mensaje de acceder - aceptar puede incluir un atributo de vendedor específico MS - MPPE - Recv - Key (por ejemplo, tal y como se especifica en la RFC 2548 de la IETF), que contiene la clave precompartida del MN 410. La clave precompartida puede ser utilizada durante las BU y BA protegidas de no IPsec por el MN 410 y el HA 430 visitante, tal y como se describe con mayor detalle más adelante. En el caso de que el MN 410 autentique con el CHAP (tal y como se describe en la etapa 651 anterior), la clave precompartida del MN 410 puede ser calculada como sigue:

PRF (MN - HAAA_Shared_Secret, CHAP_Challenge, NAI). La función pseudoaleatoria (PRF) puede ser un HMAC. El NAI puede ser un identificador de acceso a red del MN 410.

El “MN-HAAA_Shared_Secret” puede ser suministrado de antemano tanto en el MN 410 como en el servidor 440 del AAA local.

En formas de realización alternativas, la etapa 552 en el diagrama 500 de flujo de llamadas de la FIG. 5 se puede llevar a cabo, por ejemplo, en lugar de las etapas 652 y 653 anteriores.

En la etapa 654, el MN 410 lleva a cabo el IPv6CP del PPP (tal y como se especifica en la RFC 2472 de la IETF) para negociar un ID de interfaz de 64 bits, cuál el MN 410 puede utilizar para configurar su dirección de enlace local de la IPv6 (tal y como se especifica en la RFC 2460 de la IETF) y la CoA (tal y como se especifica en la RFC 3775 de la IETF) por medio de una autoconfiguración de dirección sin estado (tal y como se especifica en la RFC 2462 de la IETF).

En la etapa 655, el NAS 420 envía un Anuncio de Encaminador (por ejemplo, tal y como se especifica en la RFC 2461 de la IETF) al MN 410 que contiene un prefijo /64, sobre cuál MN 410 puede utilizar para construir su CoA mediante la adición del ID de interfaz de 64 bits negociado en la etapa 654 al prefijo /64. En una forma de realización, el anuncio de encaminador puede incluir “M - flag = 0, O - flag = 1, Router Lifetime, A - flag = 1, L - flag = 0” (por ejemplo, tal y como se especifica en la RFC 2461 de la IETF). El M - flag puede ser establecido en ‘0’, indicando que el MN 410 puede utilizar la autoconfiguración de dirección sin estado para configurar su CoA. El O - flag puede establecerse en ‘1’, indicando que el MN 410 puede utilizar la DHCPv6 sin estado para configurar otros parámetros, incluyendo (pero no limitado a) la dirección del HA 430 y la HoA del MN 410, tal y como se describe con mayor detalle más adelante.

En la etapa 656, el NAS 420 selecciona una dirección del HA 430 visitante y un prefijo de la HoA /64 para el MN 410 (por ejemplo, tal y como se especifica en la RFC 3775 de la IETF). El NAS 420 puede almacenar dicha información en el servidor de la DHCPv6 sin estado.

En la etapa 657, el MN 410 utiliza el servidor de la DHCPv6 sin estado para obtener la dirección del HA 430 visitante y el prefijo de la HoA /64. En algunas formas de realización, la dirección del HA 430 visitante y el prefijo HoA /64 pueden ser almacenadas en el servidor de la DHCPv6 como opciones de información de vendedor específico (tal y como se especifica en la RFC 3315 de la IETF). A continuación, el MN 410 crea de forma dinámica su HoA utilizando el prefijo de la HoA /64 y su ID de interfaz de 64 bits (negociados en la etapa 655 anterior). Nótese que, frente a la asignación de una HoA como en la forma de realización de las FIGs. 4 y 5 anteriores, el MN 410 construye de forma dinámica su HoA en este caso.

En la etapa 658, el NAS 420 crea una entrada, la cual puede incluir el NAI del MN 410 (tal y como se especifica en la RFC 2486 de la IETF) y una clave precompartida, en el HA 430 visitante para mensajes de BU y BA protegidos no por la IPsec (por ejemplo, tal y como se especifica en el trabajo “Autenticación para la IPv6 Móvil”, borrador de la IETF, enero 2005, y “Opción de Identificador de Nodo Móvil para la IPv6 Móvil”, borrador de la IETF, diciembre 2004). El NAS 420 puede utilizar la interfaz suministrada por el vendedor del HA 430 visitante para llevar ello a cabo (por ejemplo, tal y como se especifica en la RFC 2750 de la IETF).

En la etapa 659, el MN 410 registra el enlace de su HoA y de su CoA con el HA 430 visitante para llevar a cabo una BU. Tal y como se indicó con anterioridad esta BU puede no estar protegida por la IPsec. En su lugar puede estar protegida por la opción de movilidad de autenticación MN - HA (tal y como se especifica en el trabajo “Autenticación para la IPv6 Móvil” [Authentication for Mobile IPv6”] borrador de la IETF, enero 2005) y la opción de movilidad del NAI (tal y como se especifica en el trabajo “Opción de Identificador de Nodo Móvil de la IPv6 Móvil”, [“Mobile Node Identifier Option for Mobile IVv6”] borrador de la IETF, diciembre 2004). El HA 430 visitante puede verificar su caché (por ejemplo, rellenado por el NAS 420) para asegurar que la HoA que es registrada por el MN 410 no está ya en uso (por ejemplo, por otro MN). Tras dicha confirmación, se puede permitir el registro del MN.

En la etapa 660, el HA 430 visitante lleva a cabo una DAD apoderada (por ejemplo, tal y como se especifica en las RFCs 2462 y 3775 de la IETF) a favor del MN 410, para asegurar que ningún otro nodo en el enlace del HA 330 visitante está utilizando la HoA del MN 410.

En la etapa 661, el MN 410 recibe una BA del HA 430 visitante en respuesta a su BU en la etapa 659. Tal y como se indicó con anterioridad, esta BA puede no estar protegida por la IPsec. En su lugar puede estar protegida por la opción de movilidad de autenticación MN - HA (tal y como se especifica en el trabajo "Autenticación para la IPv6 Móvil", ["Authentication for Mobile IPv6"] borrador de la IETF, enero 2005), y la opción de movilidad del NAI (tal y como se especifica en el trabajo "Opción de Identificador de Nodo Móvil para la IPv6 Móvil", ["Mobile Node Identifier Option for Mobile IVv6"] borrador de la IETF, diciembre 2004).

Formas de realización divulgadas en la presente memoria (tal y como se han descrito con anterioridad en las FIGs. 2 a 5) proporcionan algunas formas de realización de una asignación dinámica del HA y de la HoA para el MN. Hay otras formas de realización y otras implementaciones. En formas de realización alternativas, por ejemplo, diversos procedimientos (por ejemplo, configuración de enlace de datos, autenticación, configuración de la HoA y de la CoA, la asociación de seguridad de negociación, etc.) descritos con anterioridad se pueden llevar a cabo de acuerdo con otros protocolos apropiados. Así mismo, para autoconfiguración de dirección sin estado especifica en las RFCs 2462 y 2461 de la IETF, el prefijo de subred para la HoA es /64, tal y como se describió con anterioridad. En otras formas de realización, el prefijo de subred para la HoA puede tener longitudes (o formas) diferentes.

La FIG. 7 ilustra un diagrama de flujo de un proceso 700, el cual puede ser utilizado en una forma de realización para proporcionar una asignación dinámica del HA y de la HoA para un MN. La etapa 710 asigna una dirección para un HA visitante y al menos una porción de una HoA para un MN, estando el HA visitante asociado con una red visitada con la cual se conecta el MN. El término "al menos de una porción de una HoA" puede incluir una HoA (como por ejemplo en las formas de realización de las FIGs. 4 y 5 anteriores) un prefijo de la HoA (como por ejemplo en la forma de realización FIG. 6 anterior) u otra información asociada con una HoA para el MN. La etapa 720 almacena la dirección del HA visitante y al menos una porción de la HoA para el MN en un servidor (por ejemplo, el servidor de la DHCPv6 sin estado) asociado con la red visitada. La etapa 730 crea una entrada en el HA visitante en relación con el MN. En una forma de realización, la entrada puede estar asociada con una SPD para almacenar una BU, una BA y otros mensajes. En otras formas de realización, la entrada puede incluir un NAI y una clave precompartida asociada con el MN.

El proceso 700 puede, así mismo, incluir la realización de una autenticación con la red local del MN (por ejemplo un servidor de la AAA local), por ejemplo, para obtener una clave precompartida asociada con el MN. El proceso 700 puede, así mismo, incluir la transmisión de un Anuncio de Encaminador al MN en base al cual el MN puede configurar una CoA.

La FIG. 8 ilustra un diagrama de flujo de un proceso 800, el cual puede ser utilizado en una forma de realización para proporcionar una asignación dinámica del HA y de la HoA para un MN. La etapa 810 obtiene una dirección de un HA visitante y al menos una porción de una HoA de un MN a partir de una red visitada, estando el HA visitante asociado con la red visitada a la cual está conectado el MN. La etapa 820 envía una BU al HA visitante, incluyendo la BU la HoA y una CoA asociadas con el MN. La etapa 830 recibe una PA procedente del HA visitante en respuesta a la BU.

El proceso 800 puede, así mismo, incluir la configuración de la CoA, por ejemplo, en base a un Anuncio del Encaminador recibido desde la red visitada. El proceso 800 puede, así mismo, incluir la configuración de la HoA, en base, en parte, a la porción de la HoA, (por ejemplo un prefijo de la HoA) obtenida de la red visitada. El proceso 800 puede, así mismo, incluir una asociación de configuración de negociación (por ejemplo, una IPsec) con el HA visitante.

La FIG. 9 ilustra un diagrama de bloques de un aparato 900, el cual puede ser utilizado para implementar algunas formas de realización divulgadas (tal y como se describió con anterioridad). A modo de ejemplo, el aparato 900 puede incluir una unidad (o módulo) 910 de asignación de un HA configurada para asignar una dirección para un HA visitante y al menos una porción de una HoA para un MN, en la que el HA visitante está asociado con una red visitada a la cual está conectado el MN; y una unidad 920 de almacenamiento de dirección configurada para almacenar la dirección del HA visitante y al menos una porción de la HoA para el MN. En algunas formas de realización, la unidad 920 de almacenamiento de dirección puede estar asociada con un servidor (por ejemplo, un servidor de la DCHPv6 sin estado) en la red visitada. El aparato 900 puede, así mismo, incluir una unidad 930 de autenticación configurada para llevar a cabo la autenticación con la red local del MN (por ejemplo, una AAA local). El aparato 900 puede, así mismo, incluir una unidad 940 de transmisión configurada para transmitir un "Anuncio de Encaminador.

El aparato 900, la unidad 910 de asignación del HA, la unidad 920 de almacenamiento de dirección, la unidad 930 de autenticación y la unidad 940 de transmisión pueden estar acopladas a una barra colectora 950 de comunicación. Una unidad 960 de procesamiento y una unidad 970 de memoria, pueden, así mismo, estar acopladas a la barra colectora 950 de comunicación. La unidad 960 de procesamiento puede estar configurada para controlar y / o coordinar las operaciones de varias unidades. La unidad 970 de memoria puede incorporar instrucciones, por ejemplo para ser ejecutadas por la unidad 960 de procesamiento.

En algunas formas de realización el aparato 900 puede ser implementado en un NAS, u otro medio de infraestructura de red.

La FIG. 10 ilustra un diagrama de bloques de un aparato 1000, el cual puede ser utilizado para implementar algunas formas de realización divulgadas (como las descritas con anterioridad). A modo de ejemplo, el aparato 1000 puede incluir una unidad (o módulo) 1010 de recepción de dirección configurada para obtener una dirección de un HA visitante y al menos una porción de una HoA para un MN procedente de una red visitada, donde el HA visitante está asociado con la red visitada a la cual está conectado el MN; y una unidad 1020 de enlace configurada para enviar una BU al HA visitante, incluyendo la BU la HoA y una CoA asociadas con el MN. El aparato 1000 puede, así mismo, incluir una unidad 1030 de configuración de dirección operativa para configurar la CoA, por ejemplo, en base en parte a un Anuncio de Encaminador recibido de la red visitante. En algunas formas de realización, la unidad 1030 de configuración de dirección puede, así mismo, ser operativa para configurar la HoA, en base en parte a la porción de la HoA (por ejemplo, un prefijo de la HoA) obtenida de la red visitada. El aparato 1000 puede, así mismo, incluir una unidad 1040 de autenticación configurada para llevar a cabo una autenticación con la red visitada.

En el aparato 1000, la unidad 1010 de recepción de dirección, la unidad 1020 de enlace de HA, la unidad 1030 de configuración de dirección, y la unidad 1040 de autenticación pueden estar acopladas a una barra colectora 1050 de comunicación. Una unidad 1060 de procesamiento y una unidad 1070 de memoria pueden, así mismo, estar acopladas a la barra colectora 1050 de comunicación, la unidad 1060 de procesamiento puede estar configurada para controlar y / o coordinar las operaciones de diversas unidades. La unidad 1070 de memoria puede incorporar unas instrucciones, por ejemplo, para que sean ejecutadas por la unidad 1060.

En algunas formas de realización, el aparato 1000 puede ser implementado en un MN, u otro medio de recepción de datos.

Diversas unidades / módulos de las FIGs. 9 y 10 y otras formas de realización pueden ser implementadas en hardware, software, firmware o en una combinación de estos. En una implementación de hardware, diversas unidades pueden ser implementadas dentro de uno o más circuitos integrados específicos de la aplicación (ASIC), procesadores digitales de la señal (DSP) dispositivos de procesamiento digitales de la señal (DSPDs), matrices de puertas programables sobre el terreno (FPGA), procesadores, microprocesadores, controladores, microcontroladores, dispositivos lógicos programables (PLD), otras unidades electrónicas o una combinación de estas. En una implementación de hardware, diversas unidades pueden estar implementadas con módulos (por ejemplo, procedimientos, funciones, etc.) que lleven a cabo las funciones descritas en la presente memoria. Los códigos de software pueden ser almacenados en una unidad de memoria y ejecutados por un procesador (por ejemplo, una unidad del procesador). La unidad de memoria puede ser implementada dentro del procesador o fuera del procesador, en cuyo caso puede estar comunicativamente acoplada al procesador a través de diversos medios conocidos en la técnica.

Los expertos en la materia entenderán que la información y las señales pueden ser representadas utilizando cualquiera de las diferentes técnicas y métodos. Por ejemplo, datos, instrucciones, comandos, información, señales, bits, símbolos y chips a los que se puede haber hecho referencia a lo largo de la descripción anterior, pueden ser representados mediante voltajes, corrientes, ondas electromagnéticas, campos o partículas magnéticas, campos o partículas ópticas, o cualquier combinación de estas.

Los expertos en la materia apreciarán, así mismo, que los diversos bloques lógicos, y etapas de algoritmo ilustrativas descritos con la forma de realización divulgadas en la presente memoria, pueden ser implementados como hardware electrónico, software informático o combinaciones de estos. Para ilustrar con claridad este carácter intercambiable del hardware y el software, diversos componentes, bloques, módulos, circuitos y etapas ilustrativas han sido descritas en las líneas anteriores generalmente en términos de su funcionalidad. Ya se implemente dicha funcionalidad como hardware o como software depende de la aplicación concreta y de las restricciones de diseño impuestas sobre el sistema global. Los expertos en la materia pueden implementar la funcionalidad descrita de diversas formas para cada aplicación concreta, pero dichas decisiones de implementación no deben ser interpretadas como determinantes del desviación respecto del alcance de la presente invención.

Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en conexión con las formas divulgados en la presente memoria, pueden ser implementados y llevados a cabo por un procesador de propósito general, un procesador de señal digital (DSP), un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programable sobre el terreno (FPGA) u otro dispositivo lógico programable, puerta discreta o lógica discreta, componentes de hardware discretos o cualquier combinación de estos diseñadas para llevar a cabo las funciones descritas en la presente memoria. Un procesador de propósito general puede ser un microprocesador pero, como alternativa, el procesador puede ser cualquier procesador convencional, controlador, microcontrolador o máquina de estados. Un procesador puede, así mismo, ser implementado como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y de un microprocesador, una pluralidad de microprocesadores, o uno o más microprocesadores en combinación con un DSP principal o cualquier otra configuración de este tipo.

Las etapas de este procedimiento o algoritmo descritas en conexión con las formas de realización divulgadas en la presente memoria pueden ser incorporadas directamente en hardware, en un módulo de software ejecutado por un procesador, o en una combinación de los dos. Un módulo de software puede residir en una memoria de acceso aleatorio (RAM), una memoria flash, una memoria de solo lectura (ROM), una ROM eléctricamente programable (EPROM), una ROM programable eléctricamente borrable (EEPROM), registros, disco duro, un disco extraíble, un

CD-ROM, o cualquier otra forma de medio de almacenamiento conocido en la técnica. Un medio de almacenamiento ejemplar está acoplado al procesador de forma que el procesador puede leer la información procedente de, y escribir información hacia, el medio de almacenamiento. Como alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un MN. Como alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un MN.

La descripción anterior de las formas de realización divulgadas se proporciona para permitir que cualquier experto en materia fabrique o utilice la presente invención. Diversas modificaciones a estas formas de realización resultarán evidentes sin dificultad al experto en la materia, y los principios genéricos definidos en la presente memoria, pueden ser aplicados a otras formas de realización sin apartarse del espíritu o el ámbito de la invención. Por tanto, la presente invención no pretende quedar limitada a las formas de realización mostradas en la presente memoria, sino que debe concedérsele el más amplio ámbito coherente con los principios y características novedosas divulgadas en la presente memoria.

REIVINDICACIONES

1.- Un procedimiento (700) para comunicaciones inalámbricas, que comprende:

la asignación (710) de una dirección para un agente (430) local visitante, estando el agente local visitante asociado con una red visitada a la cual está conectado un nodo móvil;

la asignación de al menos una porción de una dirección local para el nodo móvil;

la creación de una dirección local para el nodo móvil mediante la combinación de la porción de prefijo de la dirección local con un identificador de interfaz negociado con la red (230) visitada; y

la continuación con la comunicación utilizando el agente (430) local visitante y la dirección local creada.

2.- El procedimiento (700) de la reivindicación 1, que comprende, así mismo, el almacenamiento (720) de la dirección para el agente local visitante y la al menos una porción de prefijo de la dirección local para el nodo móvil en un servidor (440) asociado con la red (230) visitada.

3.- El procedimiento (700) de la reivindicación 1, que comprende, así mismo, la realización de una autenticación con una red local asociada con el nodo (410) móvil.

4.- El procedimiento (700) de la reivindicación 1, que comprende, así mismo, la transmisión de un Anuncio de Encaminador, proporcionando el Anuncio de Encaminador información para el nodo (410) móvil para configurar una dirección de apoyo.

5.- El procedimiento (700) de la reivindicación 1, que comprende, así mismo, la creación (730) de una entrada en el agente local visitante en relación con el nodo móvil.

6.- Un aparato (900) adaptado para comunicaciones inalámbricas, que comprende:

un procesador configurado para:

asignar (960) una dirección para un agente (430) local visitante, estando el agente local visitante asociado con una red visitada a la cual está conectado el nodo móvil;

asignar al menos una porción de prefijo a una dirección local para el nodo (410) móvil;

crear una dirección local para el nodo (410) móvil mediante la combinación de la porción de prefijo de la dirección local con un identificador de interfaz negociado con la red (230) visitada; y

continuar con la comunicación utilizando el agente local visitante y la dirección local creada.

7.- El aparato (900) de la reivindicación 6, en el que el procesador (960) está, así mismo, configurado para almacenar la dirección para el agente (430) local visitante y la al menos una porción de prefijo de la dirección local para el nodo móvil en un servidor asociado con la red visitada.

8.- El aparato (900) de la reivindicación 7, en el que el servidor incluye un servidor de protocolo de configuración dinámica de huesped (DHCP) sin estado.

9.- El aparato (900) de la reivindicación 6, en el que el procesador (960) está, así mismo, configurado para llevar a cabo una autenticación con una red local asociada con el nodo (410) móvil

10.- El aparato (900) de la reivindicación 6, en el que el procesador (960) está, así mismo, configurado para transmitir un Anuncio de Encaminador proporcionando el Anuncio de Encaminador información para el nodo móvil para configurar una dirección de apoyo.

11.- El aparato (900) de la reivindicación 6, en el que el procesador (950) está, así mismo, configurado crear una entrada en el agente (430) local visitante en relación con el nodo (410) móvil.

12.- Un medio no transitorio legible por computadora, que comprende unas instrucciones almacenadas en él que, si son ejecutadas por un procesador, provocan que el procesador ejecute un procedimiento que comprende:

la asignación de una dirección para un agente local visitante, estando el agente local visitante asociado con una red visitada a la cual está conectado un nodo móvil.
la asignación de al menos una porción de prefijo de una dirección local para el nodo móvil;
la creación de una dirección local para el nodo móvil mediante la combinación de la porción de prefijo de la dirección local con un identificador de interfaz negociado con la red visitada; y
la continuación con la comunicación utilizando el agente local visitante y la dirección local creada.

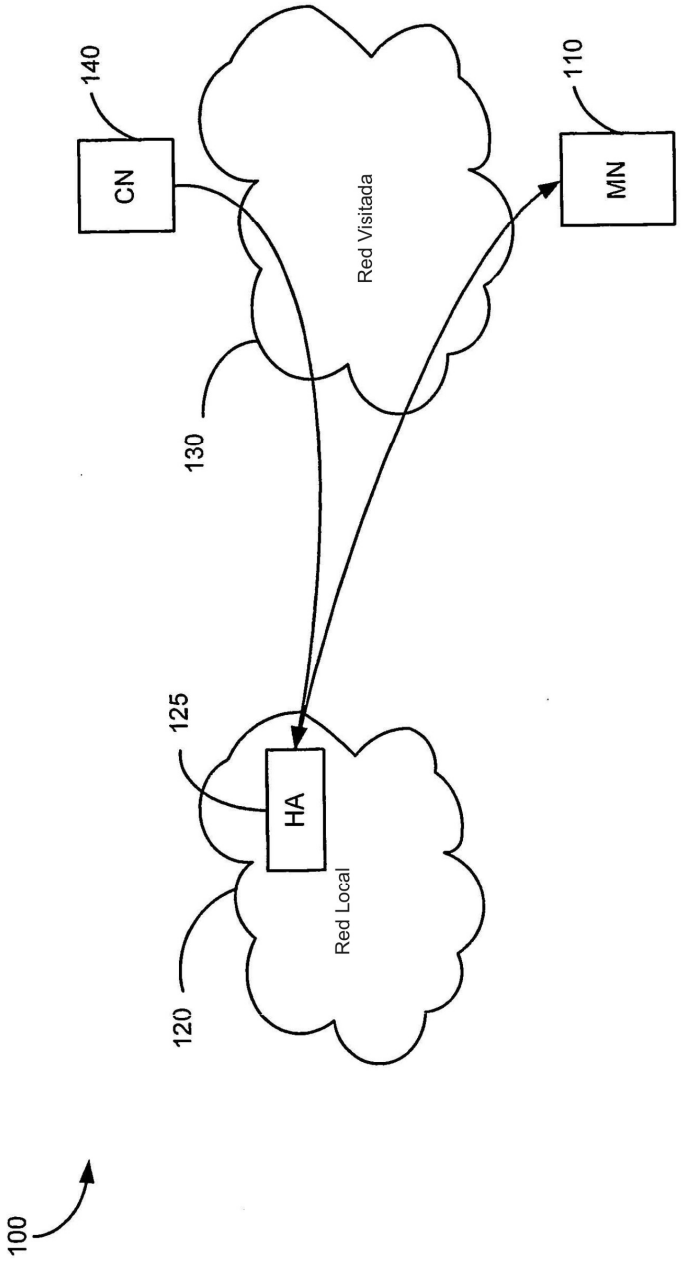

FIG. 1

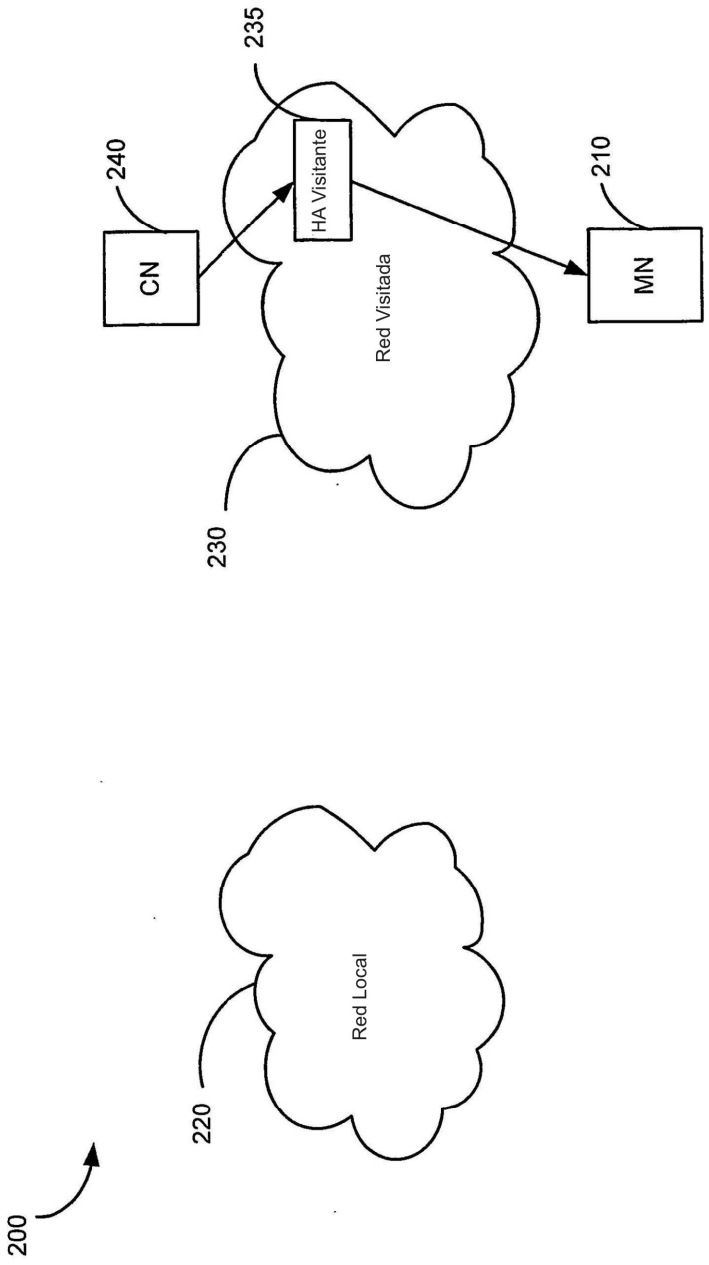
200
220
Red Local
230
Red Visitada
235
HA Visitante
240
CN
210
MN

FIG. 2

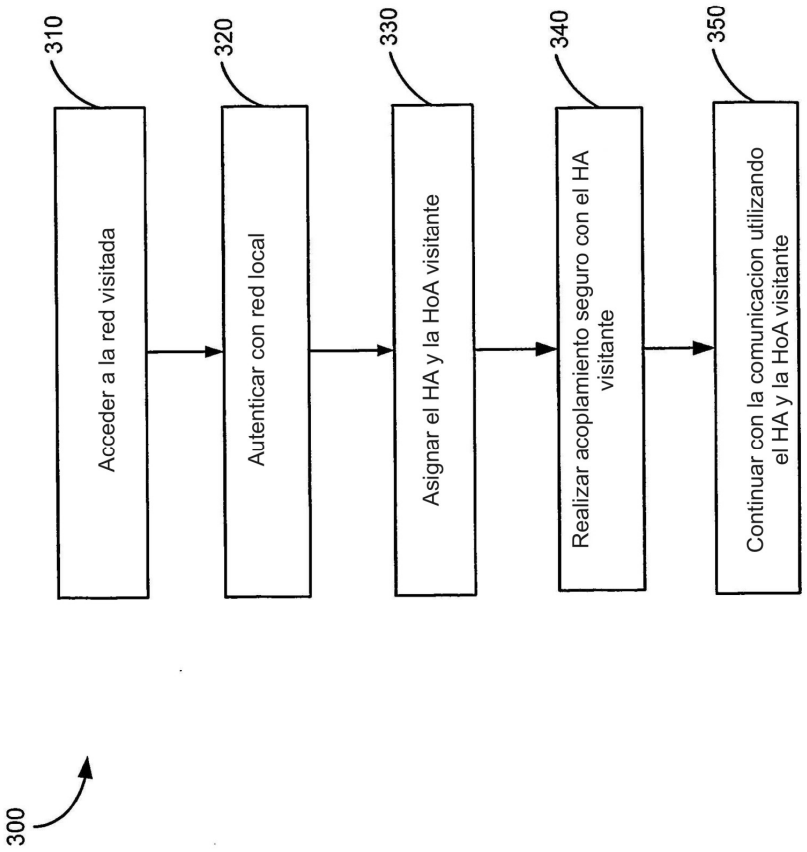
300
310
Acceder a la red visitada
320
Autenticar con red local
330
Asignar el HA y la HoA visitante
340
Realizar acoplamiento seguro con el HA visitante
350
Continuar con la comunicacion utilizando el HA y la HoA visitante

FIG. 3

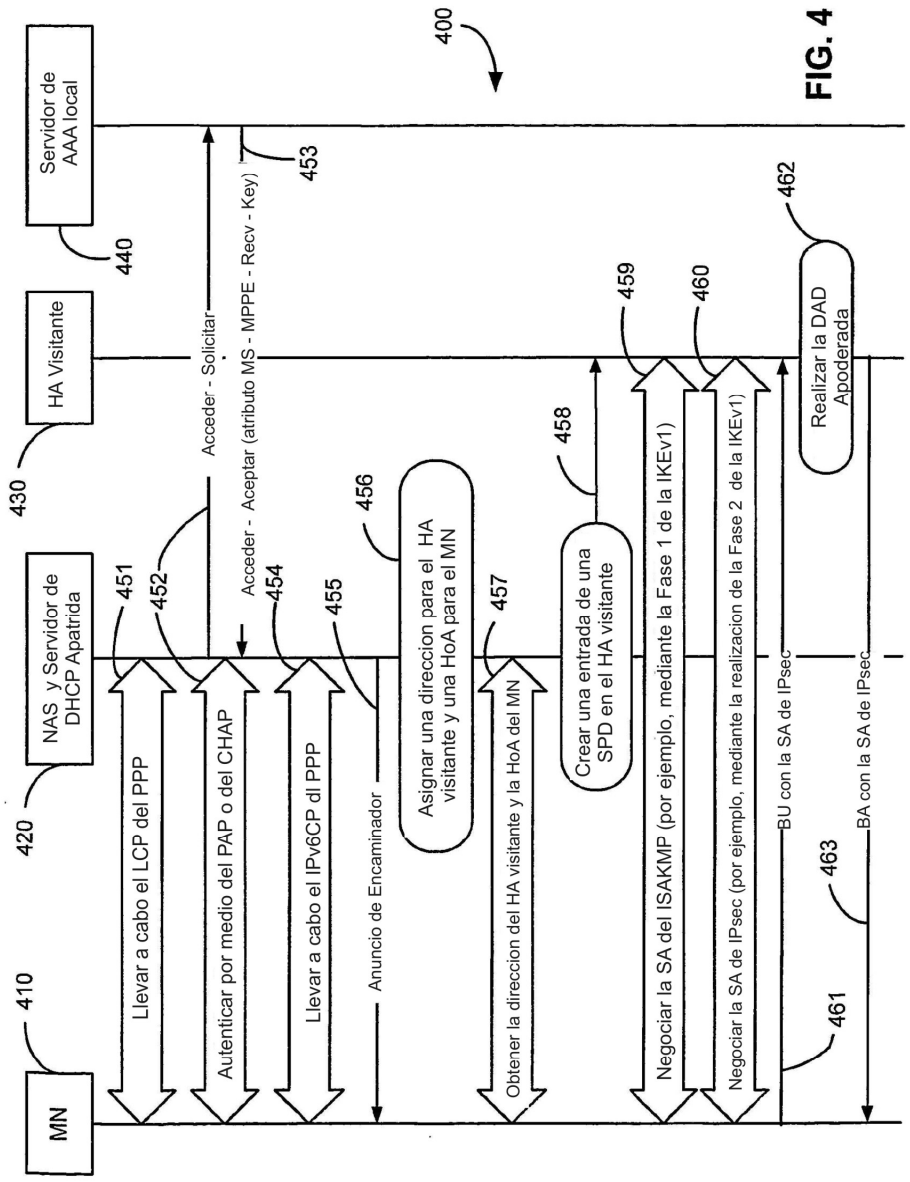
400
MN
410
NAS y Servidor de DHCP Apatrida
420
HA Visitante
430
Servidor de AAA local
440
Llevar a cabo el LCP del PPP
451
Autenticar por medio del PAP o del CHAP
452
Acceder - Solicitar
Acceder - Aceptar (atributo MS - MPPE - Recv - Key)
453
Llevar a cabo el IPv6CP dl PPP
454
Anuncio de Encaminador
455
Asignar una direccion para el HA visitante y una HoA para el MN
456
Obtener la direccion del HA visitante y la HoA del MN
457
Crear una entrada de una SPD en el HA visitante
458
Negociar la SA del ISAKMP (por ejemplo, mediante la Fase 1 de la IKEv1)
459
Negociar la SA de IPsec (por ejemplo, mediante la realizacion de la Fase 2 de la IKEv1)
460
Realizar la DAD Apoderada
462
BU con la SA de IPsec
461
BA con la SA de IPsec
463

FIG. 4

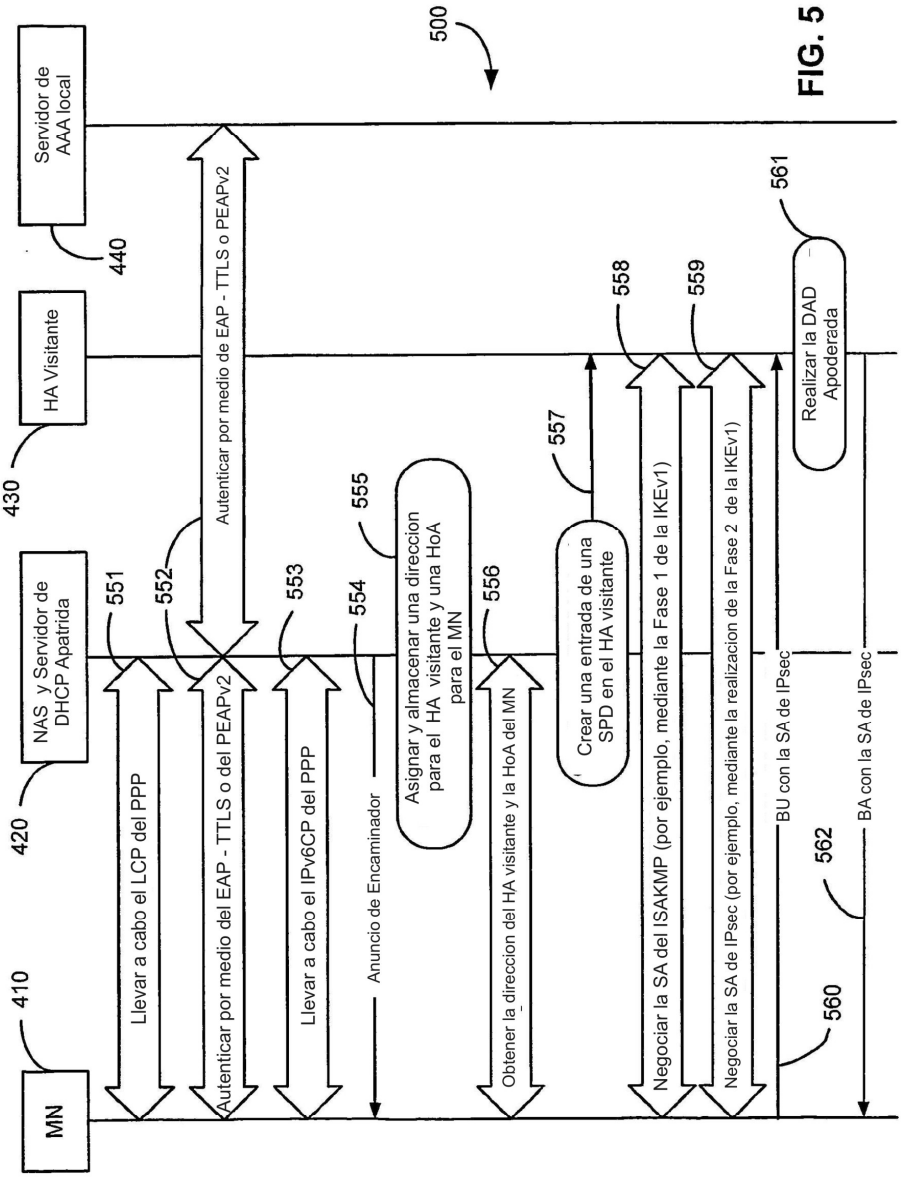
500
Servidor de AAA local
440
HA Visitante
430
NAS y Servidor de DHCP Apatrida
420
MN
410
Autenticar por medio de EAP - TTLS o PEAPv2
Llevar a cabo el LCP del PPP
Autenticar por medio del EAP - TTLS o del PEAPv2
Llevar a cabo el IPv6CP del PPP
Anuncio de Encaminador
Asignar y almacenar una direccion para el HA visitante y una HoA para el MN
Obtener la direccion del HA visitante y la HoA del MN
Crear una entrada de una SPD en el HA visitante
Negociar la SA del ISAKMP (por ejemplo, mediante la Fase 1 de la IKEv1)
Negociar la SA de IPsec (por ejemplo, mediante la realizacion de la Fase 2 de la IKEv1)
Realizar la DAD Apoderada
BU con la SA de IPsec
BA con la SA de IPsec
551
552
553
554
555
556
557
558
559
560
561
562

FIG. 5

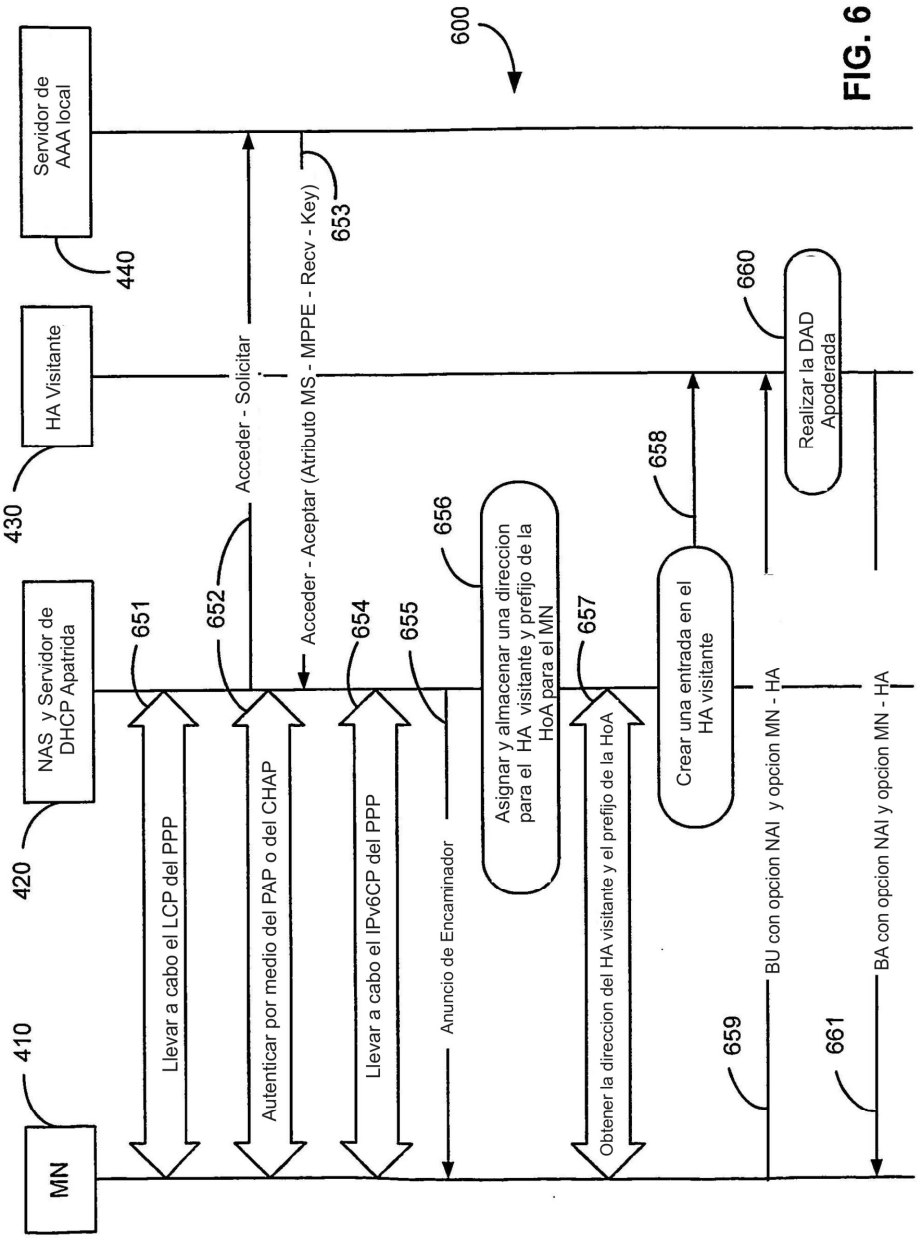
600
Servidor de AAA local
440
HA Visitante
430
NAS y Servidor de DHCP Apatrida
420
MN
410
Acceder - Solicitar
Acceder - Aceptar (Atributo MS - MPPE - Recv - Key)
653
660
Realizar la DAD Apoderada
658
656
Asignar y almacenar una direccion para el HA visitante y prefijo de la HoA para el MN
657
651
652
654
655
Crear una entrada en el HA visitante
Llevar a cabo el LCP del PPP
Autenticar por medio del PAP o del CHAP
Llevar a cabo el IPv6CP del PPP
Anuncio de Encaminador
Obtener la direccion del HA visitante y el prefijo de la HoA
BU con opcion NAI y opcion MN - HA
BA con opcion NAI y opcion MN - HA
659
661

FIG. 6

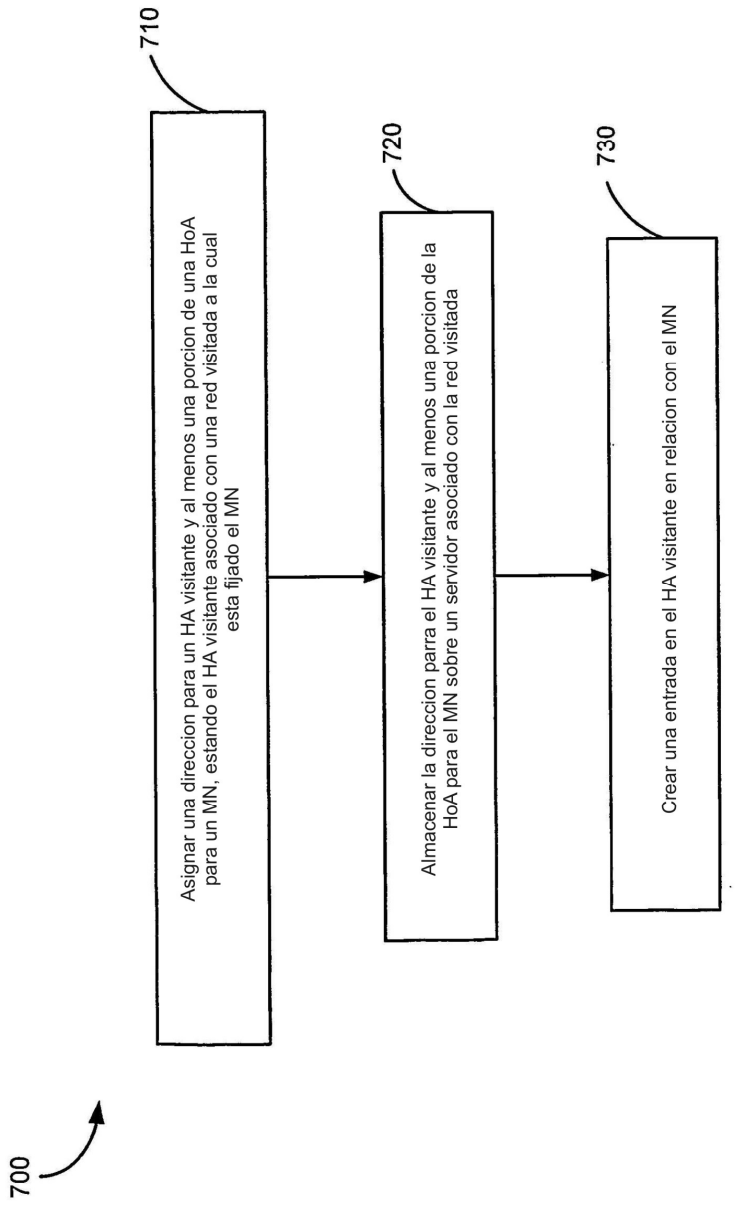
700
710
Asignar una direccion para un HA visitante y al menos una porcion de una HoA para un MN, estando el HA visitante asociado con una red visitada a la cual esta fijado el MN
720
Almacenar la direccion parra el HA visitante y al menos una porcion de la HoA para el MN sobre un servidor asociado con la red visitada
730
Crear una entrada en el HA visitante en relacion con el MN

FIG. 7

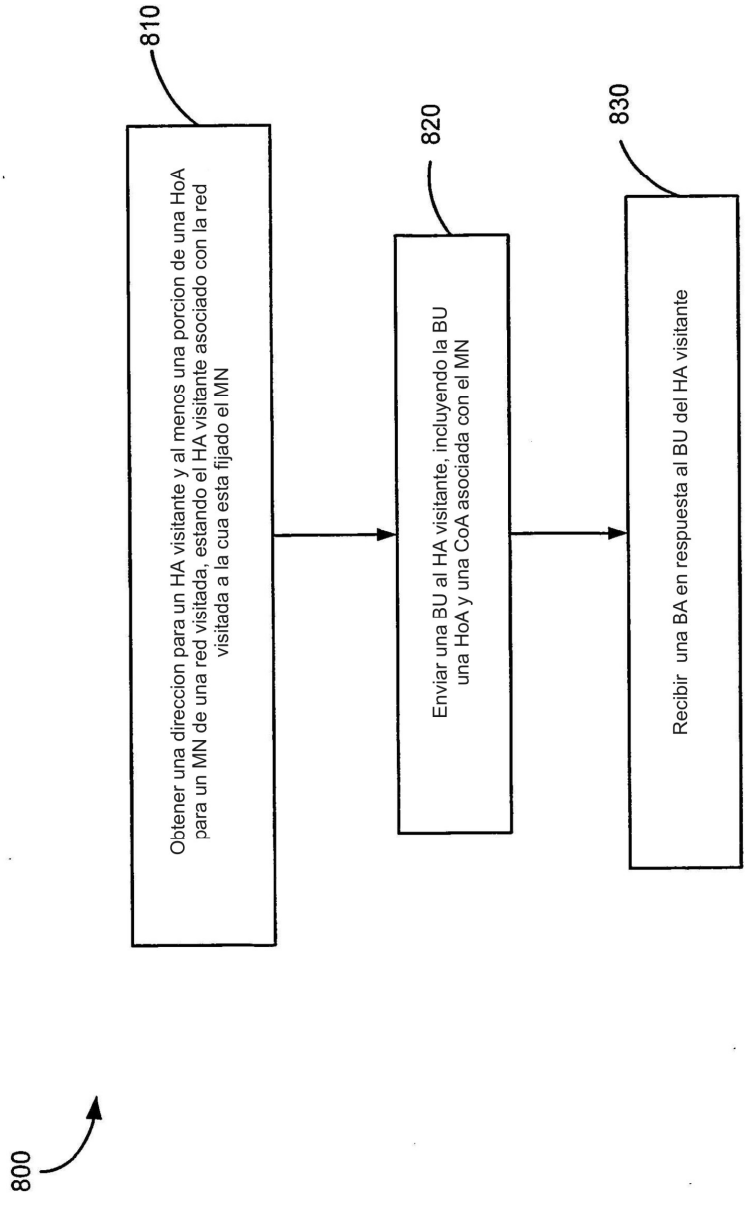
800
810
Obtener una direccion para un HA visitante y al menos una porcion de una HoA para un MN de una red visitada, estando el HA visitante asociado con la red visitada a la cua esta fijado el MN
820
Enviar una BU al HA visitante, incluyendo la BU una HoA y una CoA asociada con el MN
830
Recibir una BA en respuesta al BU del HA visitante

FIG. 8

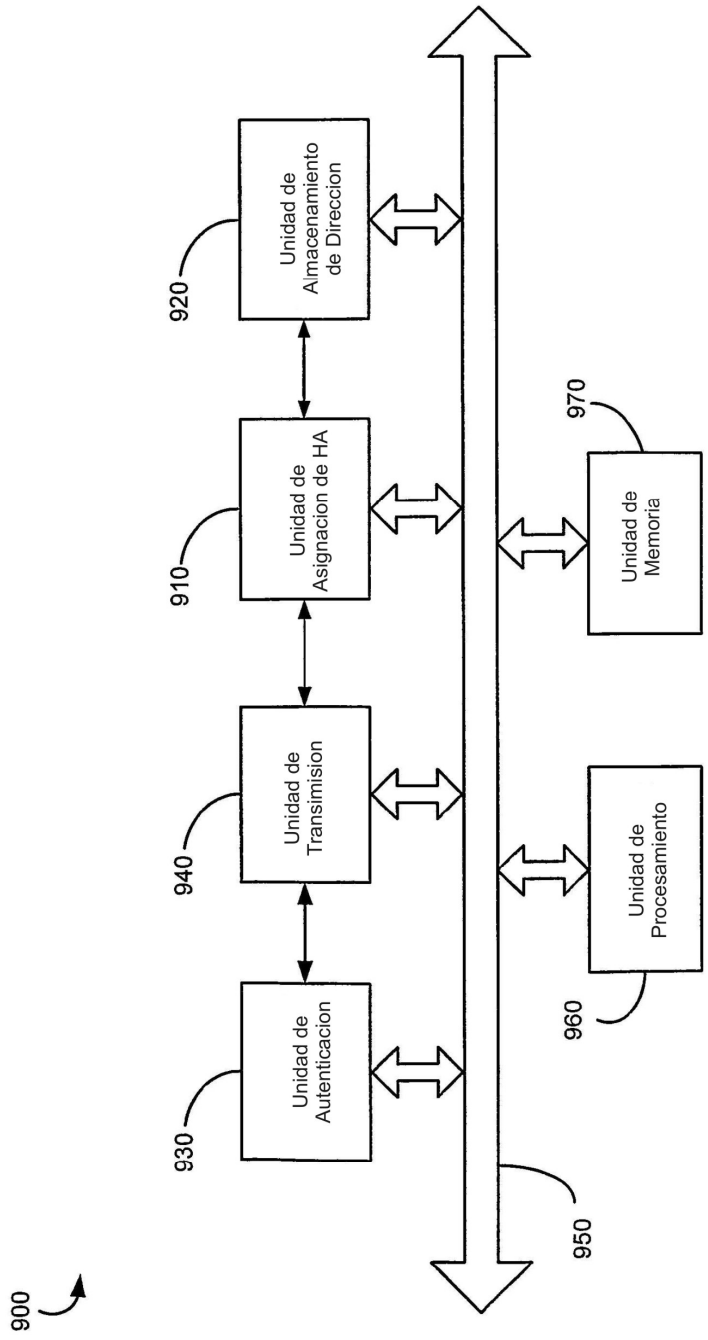
900
920
Unidad de Almacenamiento de Direccion
910
Unidad de Asignacion de HA
940
Unidad de Transimision
930
Unidad de Autenticacion
950
970
Unidad de Memoria
960
Unidad de Procesamiento

FIG. 9

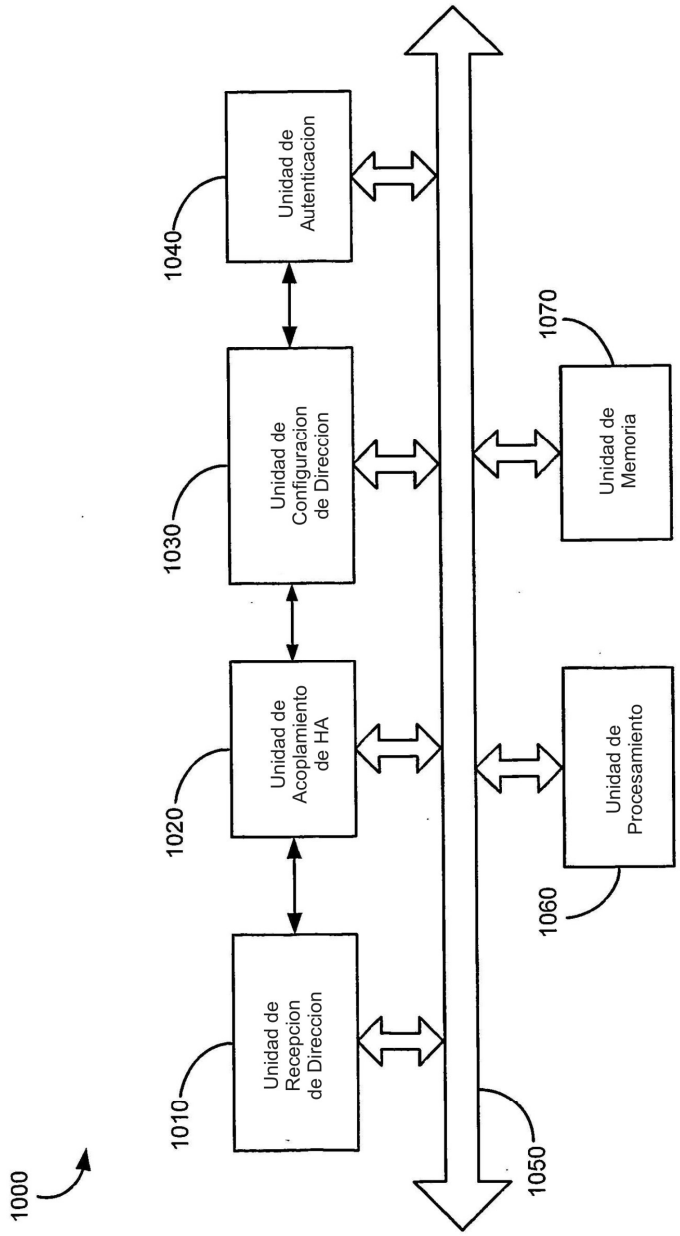
1000
1010
Unidad de Recepcion de Direccion
1020
Unidad de Acoplamiento de HA
1030
Unidad de Configuracion de Direccion
1040
Unidad de Autenticacion
1050
1060
Unidad de Procesamiento
1070
Unidad de Memoria

FIG. 10