(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 376 991**

(51) Int. CI.:
H04W 36/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09744587 .8**
(96) Fecha de presentación: **29.05.2009**
(97) Número de publicación de la solicitud: **2151142**
(97) Fecha de publicación de la solicitud: **10.02.2010**

(54) Título: **Procedimientos y aparatos para el envío de paquetes de datos entre nodos móviles**

(30) Prioridad:
02.06.2008 ES 200801653

(45) Fecha de publicación de la mención BOPI:
21.03.2012

(45) Fecha de la publicación del folleto de la patente:
21.03.2012

(73) Titular/es:
MEDIA PATENTS, S. L.
AV. DE ROMA 159, 3º 2ª
08011 BARCELONA, ES

(72) Inventor/es:
FERNÀNDEZ GUTIÉRREZ, Àlvaro

(74) Agente/Representante:
Zea Checa, Bernabé

DESCRIPCIÓN

Procedimientos y aparatos para el envío de paquetes de datos entre nodos móviles.

La invención se refiere a procedimientos y sistemas utilizados para transmitir paquetes de datos entre un nodo móvil y un segundo nodo dentro de una red de datos.

ESTADO DE LA TÉCNICA

"IP Móvil" *("Mobile IP"*) es un conjunto de protocolos del IETF que permiten a un dispositivo móvil que se comunica utilizando paquetes *IP* moverse y usar diferentes enrutadores (*routers*) en diferentes redes de datos a medida que se mueve. El término común para referirse a un dispositivo móvil es "Nodo Móvil" (*Mobile Node*).

Los dos principales protocolos IP Móvil actualmente en uso se denominan "*Mobile IPv4"* (IPv4 Móvil) y "*Mobile IPv6"* (IPv6 Móvil), que usan direcciones IP del tipo IPv4 y IPv6, respectivamente.

El protocolo "*IP Mobility Support for IPv4"* (de aquí en adelante, "*Mobile IPv4*") se describe en las especificaciones RFC 3344 (*Request for Comments 3344*), publicadas en línea por el IETF (*Internet Engineering Task Force*), C. Perkins, Agosto del 2002, actualmente disponibles en línea en http://www.ietf.org./rfc/rfc3344.txt.

El protocolo *"Mobility Support for IPv6"* (de aquí en adelante, "MIPv6" o "Mobile IPv6") se describe en las especificaciones RFC 3775, publicadas en línea por el IETF, D. Johnson et al., Junio del 2004, actualmente disponibles en línea en http://www.ietf.org/rfc/rfc3775.txt.

Una breve explicación de una operación en IP Móvil se describe a continuación.

Un "Nodo Móvil" puede tener dos direcciones IP: una dirección permanente denominada "*Home Address"*, y una dirección dinámica denominada "*Care-of-Address" (CoA),* que es una dirección asociada con la red que el Nodo Móvil está visitando en cada momento.

Un dispositivo denominado "*Home Agent"* (Agente Doméstico) almacena la información de los Nodos Móviles cuya dirección IP permanente pertenece a la misma red que el *Home Agent*. Cuando el Nodo Móvil está en su red permanente no necesita usar los servicios de movilidad.

Cuando un nodo de la red, al que se le suele denominar *Correspondent Node* desea enviar paquetes IP a un Nodo Móvil que se encuentra en una red remota, utiliza la dirección permanente del Nodo Móvil *(es decir,* la *Home Address*), para enviar los paquetes IP. Estos paquetes IP son interceptados por el *Home Agent* que encapsula los paquetes añadiéndoles una nueva cabecera IP y los reenvía por un túnel a la dirección *CoA* de la red remota en la que se encuentra el Nodo Móvil.

Para encapsular y enviar los paquetes por un túnel, el *Home Agent* y el Nodo Móvil pueden utilizar varios protocolos, incluyendo por ejemplo el protocolo "*IP Encapsulation within IP*", descrito en las RFC 2003 publicadas en línea por la IETF, Perkins et. al, Octubre de 2003, actualmente disponible en línea http://www.ietf.org/rfc/rfc2003.txt.

En *Mobile IPv4,* un dispositivo llamado "*Foreign Agent"* (Agente Externo), que es un enrutador que presta servicios de movilidad al Nodo Móvil, puede ser utilizado en la red remota. *Foreign Agents* no existen en *Mobile IPv6.*

En *Mobile IPv4*, un Nodo Móvil puede obtener su IP CoA de dos formas distintas. La primera forma es mediante un *Foreign Agent.* La dirección CoA obtenida de esta manera se denomina "*Foreign Agent Care-of-Address"* (*Foreign Agent CoA*). En este caso, la dirección IP del Nodo Móvil es una dirección IP del *Foreign Agent*. Varios Nodos Móviles pueden utilizar la misma *Foreign Agent CoA*. El *Foreign Agent* es el final del túnel. Cuando el *Foreign Agent* recibe un paquete IP dirigido al Nodo Móvil, el *Foreign Agent* retira el encapsulado y entrega el paquete original al Nodo Móvil.

La segunda forma mediante la cual un Nodo Móvil en *Mobile IPv4* puede obtener una dirección CoA no incluye la utilización de un *Foreign Agent*. El Nodo Móvil puede obtener una dirección *IP* directamente de la red remota, por ejemplo mediante el uso del protocolo *Dynamic Host Configuración (DHCP)* (Protocolo de Configuración Dinámica de Host) y asociar la dirección IP a uno de los interfaces de red del Nodo Móvil. Las direcciones obtenidas de esta manera son denominadas "*Co-located Care-of-Addresses"* (*CCoA*). Este procedimento tiene la ventaja de permitir al Nodo Móvil funcionar sin la necesidad de un *Foreign Agent*. Cuando el Nodo Móvil utiliza una *CCoA*, el Nodo Móvil es el final del túnel y cuando recibe un paquete del *Home Agent* retira el encapsulado y recupera el paquete original.

Cuando un Nodo Móvil se encuentra fuera de su red permanente y desea enviar paquetes IP a un *Correspondent Node*, el Nodo Móvil puede enviarlos de varias formas descritas a continuación.

Una forma, común tanto para *Mobile IPv4* como para *Mobile IPv6,* es encapsular los paquetes destinados al *Correspondent Node* y enviarlos primero al *Home Agent* a través de un túnel, de manera que el *Home Agent* pueda

enviarlos al *Correspondent Node*. Este procedimiento se denomina *Reverse Tunneling* (Encapsulado Inverso) y su uso en *Mobile IPv4* está descrito en las RFC 3024, G. Montenegro, Enero de 2001, disponibles actualmente en línea en http://www.ietf.org/rfc/rfc3024.txt. Su uso en *Mobile IPv6* está descrito en el apartado 11.3.1 de las RFC 3775 previamente mencionadas.

Cuando el Nodo Móvil se encuentra en una red remota puede también enviar directamente los paquetes IP al *Correspondent Node* de formas diferentes sin que pasen por el *Home Agent*.

En *Mobile IPv4*, un Nodo Móvil puede enviar los paquetes IP directamente al *Correspondent Node* utilizando la *Home Address* como dirección de origen para dichos paquetes. Esto genera un problema con los enrutadores de la red de datos que ejecutan una técnica denominada "*ingress filtering"* que comprueba que la dirección de origen de los paquetes IP a transmitir se corresponde con una dirección IP correcta basada en la topología de la red.

Mobile IPv6 permite a un Nodo Móvil enviar paquetes *IPv6* directamente al *Correspondent Node* sin que éstos pasen a través del *Home Agent,* pero sólo cuando el Nodo Móvil y el *Correspondent Node* han completado un proceso de registro denominado "*binding"*. En este caso se utiliza un proceso denominado "*Route Optimization"* (Optimización de Ruta), que evita problemas con los enrutadores que utilizan "*ingress filtering"*. Una descripción detallada se encuentra en las RFC 3375 antes mencionadas.

Uno de los problemas que debe afrontar la tecnología IP Móvil es la seguridad. Hay numerosos documentos de la IETF que describen protocolos de seguridad y muchos de ellos están interrelacionados.

Las especificaciones RFC 3776 tituladas "*Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents*", describen los mecanismos de seguridad recomendados inicialmente por la IETF para su uso en *Mobile IPv6*. Estas especificaciones están publicadas en línea por la IETF, J. Arkko et. al., Junio de 2004, y actualmente están disponibles en línea en http://www.ietf.org/rfc/rfc3776.txt.

En 2005, la IETF actualizó la arquitectura de los sistemas que utilizan *IPsec*. La nueva arquitectura está descrita en las especificaciones RFC 4301 publicadas en línea por la *IETF*, S.Kent et. al, Diciembre de 2005, actualmente disponible en línea en http://www.ietf.org/rfc/4301.txt.

Debido a que la implementación de *IPsec* es compleja y genera algunos problemas, la *IETF* publicó en el año 2006 un documento describiendo otro mecanismo de autenticación para *Mobile IPv6* más sencillo y similar al que utiliza *Mobile IPv4*. El documento se titula, "*Authentication Protocol for Mobile IPv6*", descrito en las especificaciones *RFC* 4285 publicadas en línea por la *IETF*, A. Patel et. al. Enero de 2006, actualmente disponible en línea en http://www.ietf.org/rc/rfc4285.

Existe también una actualización de las *RFC* 3776, titulada "*Mobile IPv6 Operation with IKEv2 and the revised IPsec architecture*". Son las especificaciones *RFC* 4877 publicadas en línea por la *IETF*, V. Devarapalli et. al., Abril del 2007, actualmente disponible en línea en http://www.ietf.org/rfc/rfc4877.

Aunque la seguridad de los protocolos *IP* Móvil se basa en el establecimiento de una "Asociación de Seguridad" (*Security Association*) entre el Nodo Móvil y el *Home Agent*, la mayoría de empresas de telecomunicaciones y proveedores de acceso a Internet utilizan infraestructuras *AAA* (*Authentication, Autorization and Accounting*), (Autenticación, Autorización y Registro) para gestionar los accesos a Internet de sus clientes. Como resultado, en los últimos años se han modificado los protocolos *Mobile IPv4* y *Mobile IPv6* para que puedan funcionar con servidores *AAA* y que sean estos servidores los que se encarguen de gestionar la autenticación, la autorización y el registro de los dispositivos que usan los protocolos *Mobile IPv4* y *Mobile IPv6*.

La *IETF* ha definido dos protocolos de servidores *AAA* denominados *RADIUS* y *DIAMETER (*RADIO y DIAMETRO*)*.

RADIUS (*Remote Authentication Dial In User Service*) está descrito en las especificaciones *RFC* 2865 publicadas en línea por la *IETF*, C. Rigney et. al., Junio del 2000, actualmente disponible en línea en htpp://www.ietf.org/rfc/rfc2865.txt.

DIAMETER está descrito en las especificaciones *RFC* 3588 publicadas en línea por la *IETF*, P. Calhoun et. al., Septiembre del 2003, actualmente disponible en línea en http://www.ietf.org/rfc/rfc3588.txt.

El uso de servidores *AAA* con *Mobile IPv4*, está descrito en las especificaciones *RFC* 3957 publicadas en línea por la *IETF*, C. Perkins et.al., Marzo del 2005, actualmente disponible en línea en http://www.ietf.org/rfc/rfc3957.txt.

Otro problema que debe solucionar la tecnología *IP* Móvil está relacionado con un proceso que ocurre cuando un Nodo Móvil cambia de un enrutador a otro. Este proceso de cambio de enrutador se denomina "*handover*". Cuando un Nodo Móvil cambia de un primer enrutador a un segundo enrutador es conveniente realizar el cambio de la forma más rápida posible para evitar la inhabilitación del Nodo Móvil para el envío o recepción de paquetes *IP* durante un período de tiempo (por ejemplo, unos pocos segundos). También es necesario diseñar algún mecanismo que evite

que se pierdan los paquetes *IP* que llegan al primer enrutador cuando el Nodo Móvil ya no está conectado al primer enrutador. Por ejemplo, en una aplicación de Voz sobre *IP* (*VoIP*), una latencia o retraso de unos pocos segundos en la recepción y reenvío de paquetes es inaceptable.

Para solucionar los problemas asociados al "*handover"*, la *IETF* ha publicado dos documentos que proponen diferentes soluciones. Estos documentos se titulan *FHMIPv6* y *HMIPv6* y se citan a continuación.

El documento titulado *"Fast Handover for Mobile IPv6" (FHMIPv6)* está descrito en las especificaciones *RFC* 4068 publicadas en línea por la *IETF*, R. Koodli, Julio de 2005, actualmente disponibles en línea en htttp://www.ietf.org/rfc/rfc4068.txt.

El documento titulado "*Hierarchical Mobile IPv6 Mobility Management" (HMIPv6)* está descrito en las especificaciones *RFC* 4140 publicadas en línea por la IETF, H. Soliman et. al., Agosto de 2005, actualmente disponibles en línea en http://www.ietf.org/rfc/rfc4140.txt.

Sin embargo, estas dos soluciones a los problemas de latencia previamente explicados que se generan durante en el proceso de "*handover"* son sólo soluciones parciales y todavía siguen existiendo problemas de retrasos cuando un Nodo Móvil cambia de un enrutador a otro. La presente invención permite realizar el proceso de *"handover*" de una forma mejorada, reduciendo la latencia en dicho proceso.

La solicitud de Patente Estadounidense (*U.S. Patent Application*) publicada como US2007/0177550A1 describe un procedimiento para proveer servicios de red privada virtual (*virtual prívate network, VPN*) a un Nodo Móvil (MN) en una red *IPv6* y una puerta de enlace o pasarela (*gateway*) que usa el mismo.

DESCRIPCIÓN DE LA INVENCIÓN

La invención tiene como objetivo principal proporcionar un sistema mejorado de comunicaciones para redes de datos que contienen nodos móviles.

La invención está definida por el contenido de la reivindicación 1.

Con la intención de conseguir este objetivo, se han desarrollado procedimientos para su utilización en una red de datos para transmitir paquetes de datos entre un nodo móvil y un segundo nodo conectado a la red de datos. El nodo móvil está conectado a un primer enrutador y comprende una primera asociación de seguridad con otro nodo conectado a la red de datos. Como resultado de un cambio de localización geográfica, por ejemplo, el nodo móvil se conecta a un segundo enrutador y comienza a transmitir paquetes de datos a otro nodo a través del segundo enrutador en vez de a través del primer enrutador. Durante al menos un periodo inicial de tiempo después de la transmisión de paquetes de datos a través del segundo enrutador, los paquetes de datos transmitidos desde el nodo móvil incluyen datos iniciales que permite la identificación del nodo móvil por parte del otro nodo. En la misma o en una realización alternativa, el nodo móvil usa la primera asociación de seguridad con el otro nodo durante el período de tiempo inicial que permite al nodo de la red que recibe los paquetes de datos verificar la fuente e integridad de dichos paquetes de una forma segura.

En una realización preferida, los paquetes de datos son paquetes *IP* (*Internet Protocol*).

En otra realización, la invención considera que los paquetes *IP* enviados por el nodo móvil a través del segundo enrutador pueden ser encapsulados en paquetes *IP* que usan la dirección *IP* del *Home Agent* como su dirección *IP* de destino.

En otra realización preferida, el *Home Agent* establece una asociación entre la dirección *IP* del segundo enrutador que está siendo usada por el nodo móvil y los datos iniciales que identifican al nodo móvil, y almacena esta asociación en la memoria del *Home Agent*. Preferiblemente, el *Home Agent* envía así los paquetes *IP* que recibe (que son direccionados al nodo móvil), a la dirección *IP* del segundo enrutador que está siendo usada por el nodo móvil.

En otra realización, un *Home Agent* retira el encapsulado de los paquetes *IP* que recibe del nodo móvil y reenvía estos paquetes *IP* sin el encapsulado al destino final de los paquetes.

En otra realización, la invención también tiene en cuenta que los paquetes *IP* enviados por el nodo móvil a través del segundo enrutador pueden ser encapsulados en paquetes *IP* que usan como su dirección *IP* de destino una dirección *IP* del *Correspondent Node*.

En otra realización, el *Correspondent Node* establece preferiblemente una asociación entre la dirección *IP* que está siendo utilizado por el nodo móvil en el segundo enrutador y los datos iniciales que identifican al nodo móvil, y

almacena esta asociación en la memoria del *Correspondent Node*.

En otra realización, un *Correspondent Node* envía los paquetes *IP* dirigidos al nodo móvil a la a dirección *IP* del segundo enrutador usado por el nodo móvil.

En otra realización, la invención también contempla que los paquetes de datos enviados por el nodo móvil puedan tener un primer campo que indica que un segundo campo de los paquetes de datos puede ser modificado después de que los paquetes de datos hayan sido transmitidos por el nodo móvil. El nodo móvil calcula la autentificación de los paquetes de datos como si el valor del segundo campo fuera una cadena de ceros. El receptor de los paquetes *IP* detecta el primer campo que indica que un segundo campo puede haber sido modificado, y verifica la autentificación de los paquetes *IP* como si el valor de dicho segundo campo fuera una cadena de ceros.

De acuerdo con otra realización, se sugiere un procedimiento para transmitir paquetes usando una versión o extensión del protocolo *IPv4* o *IPv6 Mobile IP* entre un nodo móvil y un primer nodo en una red de datos después de que el nodo móvil haya transmitido paquetes de datos al primer nodo a través de un primer enrutador desde una primera dirección *CoA* or *CCoA* y mediante una primera asociación de seguridad con el primer nodo, comprendiendo el procedimiento el envío de paquetes de datos al primer nodo por parte del nodo móvil a través del segundo enrutador que incluyen un identificador del nodo móvil que permite al primer nodo identificar el nodo móvil como el emisor de los paquetes de datos durante un periodo inicial de tiempo después de que la transmisión de los paquetes de datos a través del segundo enrutador haya comenzado; y durante ese período de tiempo inicial, el nodo móvil que autentifica los paquetes de datos transmite al primer nodo usando la primera asociación de seguridad con el primer nodo.

Es importante considerar que la presente invención es aplicable a cualquier otro protocolo *IP* Móvil además de *IPv4* o *IPv6*.

En otra realización, la invención comprende además el nodo móvil que se registra simultáneamente con el primer nodo y la segunda dirección *CoA* or *CCoA* durante el período de tiempo inicial.

En otra realización, la invención comprende además el nodo móvil que obtiene simultáneamente una nueva asociación de seguridad con el primer nodo durante el período inicial de tiempo.

En otra realización, la invención comprende además el nodo móvil que se registra simultáneamente con el primer nodo y la segunda dirección *CoA* o *CCoA* y que obtiene una nueva asociación de seguridad con el primer nodo durante el período de tiempo inicial.

En realizaciones alternativas, el primer nodo es un *Home Agent* y/o un *Correspondent Node* del nodo móvil.

En realizaciones alternativas, el identificador del nodo móvil es la *Home Address* del nodo móvil o un identificador de acceso a la red del nodo móvil o la parte del identificador de interfaz (*Interface Identifier*) de una dirección *IP* de un nodo móvil.

En realizaciones alternativas, la primera asociación de seguridad es una Asociación de Seguridad de Movilidad y/o incluye el uso de una *Binding Management Key*.

En otra realización, la presente invención hace uso de un protocolo de autentificación que trabaja en la capa de enlace de datos o capa de nivel 2 y que permite al nodo móvil acceder al segundo enrutador antes que la segunda dirección *CoA* o *CCoA* sea autentificada por el segundo enrutador. En una realización, el protocolo de autentificación es una versión del Protocolo de Autentificación Extensible (*Extensible Authentification Protocol*).

De acuerdo con otra realización de la presente invención, el primer nodo finaliza la transmisión de los paquetes de datos al nodo móvil si el registro de la segunda dirección *CoA* o *CCoA* no se ha completado dentro del período inicial de tiempo. En otra realización, el primer nodo reinicia la transmisión de los paquetes de datos al nodo móvil cuando el registro de la dirección *CoA* or *CCoA* se ha completado.

En realizaciones alternativas de la presente invención, los paquetes de datos enviados por el nodo móvil a través del segundo enrutador son encapsulados en paquetes *IP* que comparten la misma dirección *IP* de destino con el primer nodo. En otra realización, el primer nodo es un *Home Agent*, retirando el *Home Agent* el encapsulado del paquete *IP* y reenviando los paquetes *IP* sin el encapsulado al destino final de los paquetes.

En otras realizaciones de la presente invención, el primer nodo establece una asociación entre la segunda dirección *CoA* o *CCoA* y el identificador del nodo móvil y almacena dicha asociación en una memoria del primer nodo. Esto permite al primer nodo enviar paquetes de datos a la segunda dirección *CoA* o *CCoA* del nodo móvil después de que se haya establecido una relación entre el segundo *CoA* or *CCoA* y el identificador del nodo móvil.

En todavía otra realización, los paquetes de datos enviados por el nodo móvil incluyen un primer campo de datos que indica que un segundo campo de datos en el paquete de datos es modificable después de ser enviado por el nodo móvil, autentificando el nodo móvil los paquetes de datos como si el valor del segundo campo de datos fuera una cadena de ceros. Otra realización además incluye al primer nodo que recibe los paquetes de datos y determina basándose en el primer campo de datos que el secundo campo de datos puede haber sido modificado y en respuesta el primer nodo autentifica los paquetes de datos como si el valor del segundo campo de datos fuera una cadena de ceros.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Realizaciones preferidas de la presente invención serán descritas a continuación, con referencia a las siguientes figuras, en las cuales:

Fig. 1 muestra un nodo móvil conectado dentro de una red de datos a través de un primer enrutador.

Fig. 2 muestra el nodo móvil de la Figura 1 conectado dentro de la red de datos a través de un segundo enrutador.

Fig. 3 muestra la estructura de un paquete *IP* del protocolo *Mobile IPv4* que transporta un mensaje de petición de registro.

La Fig. 4 muestra los campos encontrados en un mensaje de petición de registro del protocolo *Mobile IPv4*.

La Fig. 5 muestra un ejemplo de los campos de una de extensión de autentificación.

La Fig. 6 muestra una implementación de la presente invención.

La Fig. 7 muestra un ejemplo de un paquete *IP* encapsulado en otro paquete *IP* para su uso en una realización de la presente invención.

La Fig. 8 muestra un ejemplo de los campos del bloque de datos etiquetado "*Latency Inhibition Extension*" en una realización de la presente invención.

DESCRIPCIÓN DETALLADA

Se proporcionan mejoras en los procedimientos para la ejecución del proceso de *handover basado* en el cambio de la conexión de un nodo móvil de un enrutador a otro en una red de datos con la finalidad de reducir la latencia que se produce en el nivel 3 del modelo *OSI* (es decir, en el nivel de red de datos).

La latencia en el *handover* es el retraso en el envío y la recepción de paquetes IP que afecta al Nodo Móvil durante el proceso de *handover*. Esta latencia tiene varias causas. Hay una primera latencia a nivel de enlace de datos (nivel 2 del modelo *OSI*) y una segunda latencia a nivel de red, o nivel 3, en el que funciona el protocolo *IP*. La latencia total es la suma de la latencia de nivel 2 más la latencia de nivel 3.

La latencia de nivel 3 tiene varias causas. Entre éstas, pueden estar: obtener una nueva dirección *IP* del segundo enrutador; verificar que no hay otro nodo utilizando la nueva dirección *IP* en el segundo enrutador; enviar una petición de registro para la nueva dirección *IP* a un *Home Agent*; esperar que el *Home Agent* autentifique la petición; y esperar a que el *Home Agent* envíe una respuesta al Nodo Móvil confirmando que el Nodo Móvil ya puede empezar a utilizar la nueva dirección *IP*. La latencia de nivel 3 está por lo tanto relacionada con el proceso de registro o "*binding"* y con la seguridad.

A continuación se explican brevemente los conceptos "*Security Association"* (*SA*) (Asociación de Seguridad) y "*Mobile Security Association"* (*MSA*) (Asociación de Seguridad Móvil) así como una nueva dirección *IP* es registrada con un *Home Agent*.

Una *Security Association* es una asociación que permite lo que convencionalmente es una conexión unidireccional (*simplex connection*) entre dos dispositivos. Entonces, se pueden ofrecer servicios de seguridad al tráfico transportado a través de esta conexión. Para asegurar el tráfico en una conexión bidireccional típica, normalmente hacen falta dos *SAs* (es decir, una *SA* para cada dirección). Utilizando dos *SAs*, dos dispositivos pueden comunicarse de forma bidireccional y segura entre sí. Se considera que la conexión es "normalmente" unidireccional porque algunos protocolos especiales de la *Mobility Security Association* son también bidireccionales.

Para simplificar la explicación, las figuras aportadas muestran una *Mobility Security Association* que permite una comunicación bidireccional segura con el uso de una única *MSA* que tiene dos extremos.

Normalmente, la información que permite comunicaciones seguras está almacenada en una *SA*. Esta información incluye, por ejemplo, la longitud de las claves secretas, las propias claves secretas, los algoritmos criptográficos, los mecanismos de autentificación, los vectores de inicialización y cualquier otra pieza de información necesaria para la

comunicación segura entre los dos diferentes dispositivos. A veces se utiliza el término *SA* para referirse a la información que es almacenada en los diferentes dispositivos que utilizan la *SA* y que les permite comunicarse de forma segura. Sin embargo la *SA* es la asociación de seguridad entre los dispositivos. La información que almacena cada dispositivo es sólo una de las posibles formas de almacenar la *SA*.

La *SA* puede ofrecer varios tipos de servicios de seguridad como, por ejemplo, autenticación o encriptación y para ello puede utilizar diferentes algoritmos y protocolos de seguridad indicados en la *SA*. La *SA* también contiene la información de las claves que deben ser usadas para la comunicación segura, como por ejemplo, una clave compartida o un par de clave pública/privada y otra información que sea requerida para utilizar los servicios de seguridad.

Para establecer una *SA* entre varios dispositivos se pueden utilizar diferentes protocolos. Estos incluyen, por ejemplo, el protocolo *ISAKMP* (*Internet Security Association and Key Management Protocol*) descrito en las especificaciones *RFC* 2408 publicadas en línea por la IETF, D. Maughan et. al. Noviembre de 1998, actualmente disponibles en línea en http://www.ietf.org/rfc/rfc2408.txt.

Los dispositivos que utilizan *SAs* las almacenan en una base de datos denominada *SAD* (*SA Database*). En la base de datos *SAD* cada *SA* está asociada con un identificador denominado un "*Security Parameter Index"* (*SPI*) que permite identificar dicha *SA*. Además, cada entrada en la base de datos *SAD* debe indicar si cada *SA* debe utilizarse en función de la dirección *IP* de destino de los paquetes *IP* o en función de las direcciones *IP* de origen y destino de los paquetes.

El término *MSA,* o "*Mobility Security Association"* se utiliza en diferentes documentos de la *IETF* para referirse a las *SAs* utilizadas por los Nodos Móviles. Por ejemplo, la *RFC* 3957 que habla sobre *Mobile IPv4* y servidores *AAA*, define una *MSA* como una conexión unidireccional que permite aplicar servicios de seguridad con el protocolo *Mobile IPv4*, para el tráfico entre el Nodo Móvil y el *Home Agent*, o para el tráfico entre el Nodo Móvil y el *Foreign Agent*. Una *MSA* se define mediante las direcciones *IP* de origen y destino y el parámetro *SPI*.

La Figura 1 muestra una red de datos 100 conectada a un enrutador denominado *Home Agent* 110 y otros enrutadores 120, 130 y 140. El *Home Agent* 110 está conectado a una red doméstica 113 (*home network*) a través de una interfaz de red 112. Otros nodos 114 y 115 pueden también estar conectados a la red doméstica. Todos estos elementos conectados a la red de datos 100 pueden considerarse también como parte de la red de datos. El término "red de datos" será utilizado para referirse tanto a la red de datos 100 como a la red 100 junto con todos los otros elementos que envían paquetes de datos a través de dicha red de datos 100.

El enrutador 120 se denomina *PAR*, una abreviatura de "*Previous Access Router*". El enrutador 130 se denomina *NAR*, una abreviatura de "*Next Access Router*". Estos nombres son frecuentemente utilizados en protocolos relacionados con *IP* Móvil, como por ejemplo el protocolo *FHMIPv6* antes mencionado. Los términos son usados para aumentar la claridad.

El término Nodo Móvil se utiliza para referirse a los nodos móviles de la red por ser el término habitual que utilizan todas las *RFCs* antes mencionadas.

El Nodo Móvil 160 se comunica de forma inalámbrica 162 mediante su interfaz de red 161 con una antena 123 que está conectada al enrutador *PAR* 120. La dirección *IP* que utiliza el Nodo Móvil se denomina *CoA1* y está representada por el elemento 1610.

El Nodo Móvil registra la dirección *CoA1* con el *Home Agent* 110 y dispone una *Mobility Security Association* MSA1 con el *Home Agent* 110.

La *MSA1* que está siendo compartida por el Nodo Móvil y el *Home Agent* se representa en la Figura 1 mediante los elementos 170, 171 y 172. El elemento 171 representa la información de la *MSA1* almacenada por el *Home Agent* 110. El elemento 172 representa la información de la *MSA1* que almacena el Nodo Móvil 160. La línea discontinua 170 indica que el *Home Agent* y el Nodo Móvil pueden comunicarse de forma segura gracias a que comparten una asociación de seguridad *MSA1*. Esta línea discontinua 170 indica que existe una asociación de seguridad *MSA* entre ambos extremos de la *MSA*. Como se ha explicado anteriormente, la *MSA* puede en realidad estar formada por dos *MSA* unidireccionales, pero para mayor claridad se representa mediante una única *MSA* en la figura 1.

Gracias a la *MSA*, el *Home Agent* 110 y el Nodo Móvil 160 pueden intercambiar mensajes seguros (por ejemplo el mensaje de registro de la dirección *CoA1*). Los datos que se transmiten entre el *Home Agent* 110 y el Nodo Móvil 160 se transmiten a través del enrutador 120 y la red de datos 100.

El Nodo Móvil 160 se puede comunicar con múltiples nodos de la red mediante el uso de protocolos *IP* Móvil. Basándose en la terminología del protocolo *IP* Móvil, estos nodos han sido denominados como "*Correspondent Nodes"*.

La Figura 1 muestra un *Correspondent Node* 150 conectado a la red de datos 100 mediante el enrutador 140. El Nodo Móvil 160 y el *Correspondent Node* 150 pueden comunicarse entre sí utilizando los protocolos de *IP* Móvil. Para ello, pueden enviarse los paquetes *IP* de varias formas distintas. Una primera forma es intercambiar los paquetes *IP* a través del *Home Agent* 110. Una segunda forma consiste en que el Nodo Móvil 160 envía directamente paquetes *IP* al *Correspondent Node* y éste a su vez puede también enviar paquetes *IP* directamente al Nodo Móvil.

Aunque para mayor claridad la Figura 1 muestra un único *Correspondent Node* 150, puede haber una pluralidad de *Correspondent Nodes* comunicándose con el Nodo Móvil, ya sea directamente o a través del *Home Agent* 110.

En el protocolo *Mobile IPv6*, el Nodo Móvil y el *Correspondent Node* pueden comunicarse directamente de una forma segura mediante la utilización de una clave denominada *Kbm* o "*Binding Management Key*" que es obtenida mediante la realización de un procedimiento denominado "*Return Routability*" explicado en la sección 5.2.5 de la RFC 3775. En la Figura 1 se ha representado dicha clave secreta Kbm1 que puede ser compartida por el Nodo Móvil 160 y el *Correspondent Node* 150 mediante los elementos 180, 181 y 182. Figura 2 muestra una comunicación directa similar mediante los elementos 280, 281 y 282. De la misma forma, la Figura 6 muestra otra comunicación directa similar mediante los elementos 680, 681 y 682.

Esta clave compartida *Kbm1* no es estrictamente hablando, una *Mobility Security Association* porque el procedimiento *Return Routability* que se utiliza para crearla es menos seguro que el utilizado para crear la *MSA1*. La expresión "asociación de seguridad" será utilizada para referirse tanto a las *Mobility Security Associations* (como por ejemplo *MSA1*), como para referirse a estas claves compartidas (como por ejemplo *Kbm1*).

La Figura 2 muestra el Nodo Móvil anterior después de haber completado el proceso de *handover* para conectarse al enrutador *NAR* 230. El Nodo Móvil 260 utiliza una nueva dirección *IP* 2610 denominada *CoA2* y se comunica inalámbricamente 262 a través su interfaz de red 261 con la antena 233, la cual está conectada al enrutador 230. El Nodo Móvil ha registrado la CoA2 en el *Home Agent* 210 y dispone de una nueva *Mobility Security Association MSA2* 271, que se representa mediante la línea discontinua 270. Debido a esta *MSA2*, el Nodo Móvil 260 y el *Home Agent* 210 pueden intercambiar mensajes seguros.

Para mayor simplicidad, las Figuras 1 y 2 no indican expresamente los enrutadores denominados *Foreign Agent* que sólo son utilizados en protocolos *Mobile IPv4*. Los *Foreign Agent* pueden estar incluidos, por ejemplo, en las antenas 123 y 133 (en las antenas 223 y 233 de la Figura 2 y en las antenas 623 y 633 de la Figura 6).

A continuación se describe brevemente el proceso usado para registra una dirección *CoA* en el *Home Agent*. Los mensajes de registro son distintos para los protocolos *Mobile IPv4* y *Mobile IPv6*. En el protocolo *Mobile IPv4* el mensaje de registro de una nueva dirección *CoA* se denomina "*Registration Request*" (*RRQ)* y en el protocolo *Mobile IPv6* el mensaje de registro se denomina "*Binding Update Message*".

En ambos protocolos *Mobile IPv4* y *Mobile IPv6*, un mensaje de registro de la *CoA* que contiene la información nueva del *CoA* se envía desde el Nodo Móvil al *Home Agent* y el Nodo Móvil espera un mensaje de respuesta del *Home Agent* antes de empezar a utilizar la nueva *CoA*, es decir, antes de empezar a enviar paquetes *IP* a los posibles *Correspondent Nodes*. Los mensajes que se intercambian pueden incluir también una firma electrónica o "*hash*", de manera que tanto el *Home Agent* como el Nodo Móvil puedan comprobar la integridad de cada mensaje y autentificar al emisor.

A continuación se explica brevemente el mensaje *RRQ* utilizado en el protocolo *Mobile IPv4*. En el *Mobile IPv4*, el *Home Agent* responde al *RRQ* mediante el envío de un mensaje de respuesta al Nodo Móvil denominado "*Registration Replay*" (*RRP)*. La Figura 3 muestra el formato de un paquete *IP* 300 que transporta el mensaje "*Registration Request*" del Nodo Móvil al *Home Agent*. El Nodo Móvil puede enviar los mensajes *RRQ* directamente al *Home Agent* o bien a través de un *Foreign Agent* que los reenviará al *Home Agent*.

El paquete *IP* 300 tiene una cabecera *IP* 310 cuya dirección de origen es la dirección *IP* de la interfaz de red del Nodo Móvil que envía el mensaje. En otras palabras, utiliza la dirección *CoA*. La dirección de destino de la cabecera *IP* es normalmente la dirección *IP* del *Home Agent* o la dirección *IP* del *Foreign Agent*.

Los mensajes *Mobile IPv4* intercambiados entre el Nodo Móvil y el *Home Agent* se envían mediante un *UDP* (*User Datagram Protocol*). La Figura 3 muestra la cabecera *UDP* 320.

Después de la cabecera *UDP* 320 viene el mensaje de Petición de Registro o RRQ 330, y a continuación hay un bloque de datos denominado "*Mobile Node-to-Home Agent Authentication Extension*" o *MHAE* 340 que protege los datos *RRQ* y una parte de los datos de la propia extensión *MHAE*. La zona de datos protegida se indica mediante la línea 370.

La Figura 4, extraída de la *RFC* 3344, muestra una vista detallada de los campos del mensaje *RRQ* y aunque una explicación detallada se encuentra en el apartado 3.3 de la misma *RFC*, algunos de los campos son brevemente

explicados a continuación.

El campo "*Home Address*" es la dirección *IP* permanente del Nodo Móvil, el campo "*Home Agent*" es la dirección IP del *Home Agent* y el campo "*Care-of-Address*" es la dirección *IP CoA* que el Nodo Móvil quiere registrar con el *Home Agent.*

También hay un campo denominado "*Lifetime*" que indica el número de segundos restantes antes de la finalización del registro. Como resultado, el Nodo Móvil debe enviar mensajes tipo *RRQ* al *Home Agent* si desea mantenerse registrado. Un valor 0 en el campo *Lifetime* significa que el Nodo Móvil desea desconectarse (es decir, no estar registrado).

El campo "*Identification*" es un campo que se modifica cada vez que un mensaje es enviado. Permite asociar cada mensaje *RRQ* con su respuesta *RRP* y evita ataques de seguridad conocidos como "*Replay attacks*".

La Figura 5, extraída del apartado 3.5.2 de la *RFC* 3344, muestra el formato de la extensión *MHAE* que se añade al mensaje *RRQ* para incrementar la seguridad. El campo "*SPI*" o "*Security Parameter Index"* muestra la *MSA* (*Mobility Security Association*) que comparten el *Home Agent* y el Nodo Móvil.

El campo "*Authenticator*" sirve para proteger los datos del mensaje *RRQ*. Este campo se calcula utilizando un algoritmo de seguridad que se aplica sobre los datos del paquete *IP* empezando justo después del encabezado *UDP* y terminando justo antes del presente campo *Authenticator*. La sección 3.5.1 de la *RFC* 3344 explica en detalle cómo se calcula dicho campo *Authenticator*.

Gracias al campo *Authenticator* y a la *MSA* que comparten el Nodo Móvil y el *Home Agent*, cuando el Nodo Móvil y el *Home Agent* intercambian mensajes pueden confirmar su integridad y su procedencia de una forma segura.

La sección 3.2. de la *RFC* 3344 indica que los mensajes *RRQ* y el *Authentication Replay* deben incluir obligatoriamente la extensión de seguridad *MHAE*. Por lo tanto, el Nodo Móvil 260 de la Figura 2 no puede enviar el mensaje *RRQ* hasta que se establezca una *MSA2* con el *Home Agent*. En otras palabras, el Nodo Móvil debe establecer primero una nueva *MSA2* con el *Home Agent* y una vez obtenida la nueva *MSA2* puede iniciar el proceso de registro de la dirección *CoA2*.

El Nodo Móvil y el *Home Agent* pueden utilizar diferentes mecanismos para establecer una *MSA* como por ejemplo los protocolos denominados *Internet Key Exchange* tales como *IKEv1* o *IKEv2*. También pueden crear la *MSA* utilizando una infraestructura de tipo *AAA* como se describe en la *RFC* 3957 denominada "*Authentication, Autorization and Accounting (AAA) Registration Keys for Mobile IPv4*" de C. Perkins, et. al., Marzo del 2005, disponible en línea en http://www.ietf.org/rfc/rfc3957.txt.

Como resultado, cuando el Nodo Móvil realiza el proceso de *handover* y cambia de un enrutador a otro, debe primero obtener una nueva MSA2 con la nueva dirección CoA2. Luego el Nodo Móvil registra la nueva CoA2 con el *Home Agent*, envía un mensaje de registro al *Home Agent* y espera un mensaje de respuesta del *Home Agent* para confirmar que se ha realizado el registro correctamente. Sólo cuando el Nodo Móvil haya completado todos estos pasos podrá empezar a enviar paquetes *IP* a otros nodos (por ejemplo, *Correspondent Nodes*) de la red utilizando la dirección *CoA2*. Este proceso genera una latencia de nivel 3 (es decir, nivel de red de datos), que está asociada a los mismos procesos que la presente invención reduce o elimina completamente.

Para poder reducir o eliminar la latencia asociada con el proceso de registro de una nueva dirección *CoA* del Nodo Móvil y el establecimiento de la nueva *MSA2* sin que la seguridad se vea afectada, la presente invención modifica varias características de los protocolos *IP* Móvil. Estas modificaciones se explican a continuación.

En una realización, una característica de los protocolos IP Móvil que modifica la presente invención es el requerimiento del Nodo Móvil de registrar una nueva dirección *CoA* or *CCoA* con el *Home Agent* antes de empezar a utilizar la nueva dirección. Tal como se ha explicado anteriormente, el *Home Agent* necesita saber cuál es la *Home Address* asociada a los paquetes *IP* que el Nodo Móvil envía desde la nueva dirección *CoA2* y también necesita saber a qué dirección *CoA* debe enviar los paquetes que lleguen al *Home Agent* dirigidos al Nodo Móvil. Esta característica también se da en el protocolo *IPv6* cuando la comunicación entre el Nodo Móvil y el *Correspondent Node* se hace utilizando un proceso denominado "Optimización de Ruta" (*Route Optimization*) que permite al Nodo Móvil la opción de enviar los paquetes *IP* directamente al *Correspondent Node* sin que estos paquetes *IP* pasen a través del *Home Agent*. En este caso el Nodo Móvil debe registrar la nueva CoA2 con el *Correspondent Node* y esperar una respuesta del *Correspondent Node*.

En otra realización, una característica de los protocolos *IP* Móvil que se modifica es el proceso para registrar el Nodo Móvil con el nuevo enrutador (por ejemplo, *NAR*) en el que se considera como una petición de autorización por parte del Nodo Móvil para obtener acceso a la red a través del nuevo enrutador. Para el proceso de registro, primeramente es necesario establecer una nueva *MSA2* (*Mobility Security Association*) entre el Nodo Móvil y el *Home Agent* teniendo en cuenta la nueva *CoA2* que va a ser utilizada por el Nodo Móvil. Esto provoca un aumento de la latencia

del proceso de registro de la nueva *CoA2* ya que el Nodo Móvil no puede enviar el mensaje de registro al *Home Agent* desde la nueva dirección *CoA2* hasta que no dispone de la nueva *MSA2* asociada a la nueva dirección *CoA2* que desea utilizar.

Adicionalmente, si se utiliza un servidor *AAA* remoto para autentificar un Nodo Móvil que quiere conectarse a un enrutador, el *Home Agent* debe esperar a recibir una respuesta por parte del servidor *AAA* antes de dar autorización al Nodo Móvil para poder conectarse. Por ejemplo, el servidor *AAA* puede ser el encargado de establecer la nueva *MSA* entre el *Home Agent* y el Nodo Móvil. Esto provoca un aumento de la latencia experimentada durante el *handover*.

Este proceso de registro también afecta la Optimización de Ruta (*Route Optimization*), las comunicaciones directas entre el Nodo Móvil y el *Correspondent Node* en el protocolo *Mobile IPv6*. Cuando el Nodo Móvil y el *Correspondent Node* se comunican directamente sin enviar los paquetes *IP* a través del *Home Agent*, ambos utilizan un procedimiento de seguridad denominado "*Return Routability Procedure*" descrito en la sección 5.2 de la *RFC* 3775 para establecer una clave secreta denominada *Kbm*. Aunque dicha clave no se denomina una "*Mobility Security Association*", aporta seguridad salvaguardando las comunicaciones entre el Nodo Móvil y el *Correspondent Node*.

En la sección 11.3.1 titulada "*Sending Packets While Away from Home*" de la *RFC* 3775 se explica que si un Nodo Móvil desea enviar paquetes a un *Correspondent Node* con el que no ha establecido un proceso de registro o "*binding*", el Nodo Móvil debe enviar los paquetes a través del *Home Agent*. En otras palabras, el proceso de "*binding*" es necesario para que el Nodo Móvil pueda enviar los paquetes directamente al *Correspondent Node*. Durante este proceso de "*binding*" se utiliza un mecanismo de seguridad denominado "*return routability*", el cual también provoca una latencia de nivel 3.

La presente invención modifica una o ambas de estas dos características de los protocolos *IP* Móvil durante un período de tiempo limitado (por ejemplo, 60 segundos). Durante este período de tiempo limitado que será denominado como "Tiempo de Autorización Provisional" (*Provisional Authorization Time*), el Nodo Móvil puede enviar paquetes IP usando la nueva dirección *CoA2* del nuevo enrutador *NAR* 230, aunque no se haya realizado el proceso de registro de la dirección *CoA2* ni se haya obtenido la nueva *MSA2*.

De acuerdo con la presente invención, el proceso de obtención de la nueva MSA2 y/o el proceso de registro de la nueva *CoA2* en el *Home Agent* o en *Correspondent Node* se completan durante el "*Tiempo de Autorización Provisional*". Durante este tiempo, el Nodo Móvil envía paquetes IP utilizando la dirección *CoA2*. De esta forma, para los paquetes *IP* enviados por el Nodo Móvil, la presente invención es capaz de reducir o preferiblemente eliminar completamente la latencia causada por el proceso de registro de la nueva dirección *IP* que va a utilizar el Nodo Móvil en el *Home Agent* (o *Correspondent Node*), así como la latencia asociada a la autentificación de la petición de registro y la latencia asociada a la espera de la respuesta de la petición de registro que recibe el Nodo Móvil.

Puesto que el Nodo Móvil envía paquetes IP usando la dirección de origen *CoA2* antes de haber obtenido la *MSA2* y haber registrado la nueva *CoA2*, se generan tres problemas durante el Tiempo Provisional de Autorización (*Provisional Authorization Time*) relacionados con la comunicación con el Nodo Móvil, independientemente de si se comunican a través del *Home Agent* o de si se comunican directamente con el *Correspondent Node*. A continuación se describen estos problemas y la solución que aporta la presente invención.

Un primer problema es que el *Home Agent* que recibe los paquetes *IP* enviados por el Nodo Móvil con la nueva *CoA2* no tiene una entrada en su tabla de registro que indique qué *Home Address* se corresponde con la nueva *CoA2*. Como resultado, es necesario establecer un mecanismo que permita identificar qué *Home Address* está asociada a la dirección *CoA2* o, en otras palabras, qué Nodo Móvil está enviando los paquetes *IP* desde la dirección *CoA2* no registrada.

Un segundo problema está relacionado con la seguridad. El nodo que recibe los paquetes *IP* enviados por el Nodo Móvil durante el Tiempo Provisional de Autorización debe comprobar de una forma segura que los paquetes *IP* proceden efectivamente del Nodo Móvil 260 así como comprobar la integridad de los paquetes de datos aunque todavía no se haya establecido la asociación de seguridad *MSA2* entre el Nodo Móvil y *Home Agent* para las comunicaciones que tienen lugar a través del *Home Agent*.

Estos problemas que afectan a los protocolos *Mobile IPv4* y *Mobile IPv6* cuando el Nodo Móvil se comunica a través del *Home Agent*, también se dan en el protocolo *Mobile IPv6* cuando existe una comunicación directa entre el Nodo Móvil y el *Correspondent Node*. Mientras no se establece la clave secreta Kbm2 utilizando el procedimiento denominado "*Return Routability*", el Nodo Móvil y los *Correspondent Nodes* no pueden intercambiar mensajes seguros. Además el *Correspondent Node* desconoce cuál es la dirección *Home Address* correspondiente a los paquetes *IP* recibidos que no tienen una dirección de origen *CoA2* registrada.

El tercer problema que soluciona la presente invención es que el *Home Agent* no sabe a qué dirección *CoA* debe enviar los paquetes *IP* dirigidos al Nodo Móvil mientras el Nodo Móvil no ha registrado todavía la nueva dirección

CoA2. Lo mismo ocurre en *Mobile IPv6* con los paquetes que el *Correspondent Node* envía directamente al Nodo Móvil.

La presente invención soluciona el primer problema incluyendo un identificador del Nodo Móvil en los paquetes *IP* enviados durante el Tiempo de Autorización Provisional. Como identificador del Nodo Móvil, la presente invención puede utilizar cualquier pieza de datos que permita al nodo que recibe el paquete *IP* identificar de forma única al Nodo Móvil que envía el paquete *IP*.

Por ejemplo, en realizaciones preferidas alternativas, la presente invención usa la *Home Address,* un campo de tipo *Network Access Identifier* o los 64 bits menos significativos de la dirección *CoA2* de *IPv6* denominados "*Interface Identifier*", como el identificador del Nodo Móvil cuando estos 64 bits son iguales en las diferentes direcciones *IP* que utiliza el Nodo. Más adelante se explican con mayor detalle estos identificadores. La presente invención puede usar también cualquier otro identificador que identifique al Nodo Móvil.

La Figura 6 muestra como, en una realización, se soluciona el segundo problema relacionado con la seguridad. Para ello, se autentifican los paquetes *IP* que el Nodo Móvil 660 envía durante el "Tiempo de Autorización Provisional" desde la nueva dirección *CoA2* utilizando la *MSA1* 670 que el Nodo Móvil utilizó con la anterior dirección *CoA1* (con la referencia 170 en la Figura 1). De esta forma, el Nodo Móvil puede autentificar los paquetes IP que envía al *Home Agent* durante el Tiempo de Autorización Provisional, cuando el Nodo Móvil 660 está conectado al enrutador 630 y utiliza la nueva dirección *CoA2* y todavía no dispone de la nueva *MSA2*.

De forma similar, si el Nodo Móvil 660 se comunica directamente con el *Correspondent Node* 650 utilizando un procedimiento denominado "*Route Optimization*", el Nodo Móvil puede utilizar durante el "Tiempo de Autorización Provisional" la anterior clave *Binding Management Key* (*Kbm1* 680). Esta *Binding Management Key* se utilizó anteriormente para comunicar con el *Correspondent Node* y se obtuvo de la dirección *CoA1* mediante el procedimiento de seguridad denominado "*Return Routability*".

En la realización de la Figura 6, el Nodo Móvil 660 utiliza la antigua *MSA1*, que todavía le permite enviar paquetes autentificados al *Home Agent* 610. La asociación de seguridad *MSA1* se indica mediante la línea discontinua 670 que une el *Home Agent* con el Nodo Móvil.

En los protocolos Mobile IP estándar el proceso de registro equivale a un proceso de autorización requerido para utilizar un recurso de la red (por ejemplo, la nueva dirección *CoA2* del enrutador 630). Por este motivo, en los protocolos *Mobile IP* estándar el Nodo Móvil debe utilizar una nueva *MSA2* con el enrutador 630 incluso aunque ya dispusiera de un medio seguro para comunicarse con el *Home Agent* con la antigua *MSA1*.

Sin embargo, no es necesario que, tal como establecen los protocolos *Mobile IP* descritos en las *RFC* 3344 y *RFC* 3375, el proceso de autorización que permite que el Nodo Móvil 660 utilice la nueva dirección *CoA2* se complete durante el proceso de registro. Por ejemplo, existen diferentes protocolos de autentificación que funcionan a nivel de capa de enlace de datos o nivel 2 y es posible que el Nodo Móvil, incluso aunque no haya obtenido la dirección *CoA2* todavía, haya completado un proceso de autentificación para acceder a los recursos del enrutador 630 utilizando un mecanismo de autentificación de nivel 2.

Un ejemplo de un protocolo de autenticación que puede funcionar a nivel 2 o nivel de capa de enlace de datos es el protocolo "*Extensible Authentication Protocol*" (EAP) descrito en las especificaciones *RFC* 3748, B. Aboba et. al. Junio de 2004, actualmente disponibles en línea en http://www.ietf.org/rfc/rfc3748.txt.

El protocolo *EAP* inicialmente se desarrolló para funcionar junto con el protocolo *PPP* ("*Point to Point Protocol*") para autentificar los accesos a una red de datos desde un módem. Desde el desarrollo inicial del protocolo *EAP*, este se ha extendido de forma que actualmente *EAP* es un protocolo de autentificación de uso general que puede utilizarse de muchas formas distintas.

Como resultado, de acuerdo con un aspecto de la presente invención, no es necesario para el Nodo Móvil obtener una nueva *MSA2* antes de poder utilizar el enrutador *NAR* 630 o antes de poder enviar paquetes *IP* (por ejemplo un paquete *IP* que contiene el mensaje de registro de la nueva dirección *CoA2*), como se especifica en los protocolos IP Móvil.

De esta manera, el uso de la *MSA1* o de la *Kbm1* para autentificar los paquetes enviados por el Nodo Móvil durante el Tiempo de Autorización Provisional resuelve el segundo problema de seguridad previamente mencionado.

Volviendo a la Figura 6, también es posible que el enrutador 630 pudiera ser un enrutador que no necesita autentificar a los usuarios, como un enrutador *WIFI* de acceso abierto, a menudo denominados como "*hot spot*", y que no se requiera ningún proceso de autentificación para utilizar una dirección *IP* obtenida de dicho enrutador ya que su uso es libre para todos los usuarios que eligen conectarse a él.

Con respecto al tercer problema que impide que el *Home Agent* pueda enviar paquetes *IP* dirigidos a una dirección

Home Address no registrada, este problema se soluciona en una realización de la presente invención si los paquetes *IP* que envía el *Mobile Node* a través del *Home Agent* durante el Tiempo de Autorización Provisional incluyen una información de identificación del *Mobile Node* (como por ejemplo, la *Home Address*).

De esta forma, el *Home Agent* puede asociar la nueva dirección *CoA2* con la *Home Address* permanente y puede empezar a enviar paquetes *IP* destinados al *Mobile Node* a la nueva dirección *CoA2,* mientras el Nodo Móvil completa el proceso de registro de la nueva *CoA2*.

Para ello, el *Home Agent* detecta que un identificador está incluido en los paquetes IP recibidos de la dirección *IP* de origen *CoA2* del Nodo Móvil (por ejemplo, la *Home Address*). Además, el Nodo Móvil puede incluir una autentificación con los paquetes que asegura que es realmente el Nodo Móvil que está utilizando en ese mismo instante la dirección *CoA2*. Para ello, el Nodo Móvil también puede utilizar la *MSA1* para autentificar o encriptar los paquetes *IP* que envía mientras obtiene la *MSA2*. De este modo, se reduce o preferiblemente se elimina la latencia asociada con los paquetes *IP* recibidos por el *Mobile Node* desde el *Home Agent*.

Esta misma solución es también efectiva cuando el *Correspondent Node* 650 desea enviar paquetes *IP* directamente al Nodo Móvil 660 y el Nodo Móvil todavía no ha registrado la nueva dirección *CoA2* con el *Correspondent Node* 650. Si el *Correspondent Node* recibe un paquete *IP* desde la dirección *CoA2* que incluye la *Home Address*, el *Correspondent Node* puede asociar dicha *Home Address* con la nueva dirección *CoA2* y empezar a enviar paquetes *IP* al Nodo Móvil durante el Tiempo de Autorización Provisional.

Para incrementar la seguridad durante este proceso, si finaliza el Tiempo de Autorización Provisional sin que el Nodo Móvil haya registrado correctamente la nueva dirección *CoA2* con el *Home Agent*, éste puede dejar de transmitir paquetes provenientes o dirigidos al Nodo Móvil hasta que éste haya completado el proceso de registro para la nueva *CoA2*. Este mecanismo de seguridad también es aplicable a los paquetes *IP* que el *Correspondent Node* envía directamente al Nodo Móvil.

Alternativamente, los paquetes de datos que el Nodo Móvil envía y recibe tanto del *Home Agent* como del *Correspondent Node* pueden ser encriptados utilizando las asociaciones de seguridad *MSA1* y *Kbm1,* respectivamente.

La Figura 7 muestra una manera de implementar la presente invención en la cual los paquetes *IP* enviados por el Nodo Móvil durante el Tiempo de Autorización Provisional se encapsulan dentro de otro paquete *IP* 700 que incluye una nueva cabecera *IP* 710, un bloque de datos denominado "*Latency Inhibition Extension*" 720 y el paquete *IP* original formado por una cabecera *IP* 730 y un bloque de datos 740.

Durante el Tiempo de Autorización Provisional, cuando el Nodo Móvil desea enviar al *Correspondent Node* un paquete *IP* que contiene una cabecera *IP* 730 y un bloque de datos 740, el Nodo Móvil simplemente encapsula el paquete *IP* que incluye 730 y 740 en un nuevo paquete *IP* 700. El nuevo paquete *IP* 700 incluye la nueva cabecera 710 y el bloque de datos 720 denominado *Latency Inhibition Extension*.

La Figura 8 muestra una posible configuración del bloque de datos denominado "*Latency Inhibition Extension*" (*LIE*). Este bloque de datos tiene un campo "*LIE Type*" que indica si el bloque de datos puede ser usado para implementar la presente invención y qué tipo de datos se incluyen. Puede indicar, por ejemplo, si las direcciones *IP* que contiene son direcciones *IPv4* de 32 bits o direcciones *IPv6* de 128 bits o alguna combinación de ambas direcciones *IPv4* e *IPv6*.

El uso direcciones *IPv4* e *IPv6* combinadas es útil en los protocolos Mobile *IP* porque las tecnologías de redes móviles, como por ejemplo *3GPP*, *3GPP2* y *IMS* (*IP Multimedia Subsystem*) suelen utilizar direcciones del tipo *IPv6*. Por otro lado, las redes fijas de internet normalmente usan en la actualidad direcciones del tipo *IPv4*. El documento "*Mobile IPv6 support for dual stack Host and Routers*" (*DSMIPv6*), Hesham Soliman, Noviembre de 2007, actualmente disponible en línea en http://tools.ietf.org/html/draft-ietf-mip6-nemo-v4traversal-06, describe un ejemplo de cómo combinar el uso de direcciones *IPv4* y *IPv6* en protocolos *IP* Móvil.

La Figura 8 muestra direcciones *IP* de 32 bits pero otro tipo de direcciones también pueden ser usadas en la presente invención como resultado del campo "*LIE Type*".

El campo "*LIE Length*" indica el número de bytes que hay en el bloque de datos *LIE* 720.

El campo "*Mobile Node Identifier*" es un identificador único del Nodo Móvil. La Figura 8 muestra este campo con una longitud de 32 bits pero otras longitudes son también posibles. Este campo puede contener cualquier identificador que permita identificar de forma única el Nodo Móvil aunque incluso éste cambie de enrutador y de dirección *CoA*. Por ejemplo, puede utilizarse como identificador la dirección *IP* permanente del Nodo Móvil o la *Home Address*.

Otro posible identificador es el *Network Access Identifier* (*NAI*) descrito en las especificaciones *RFC* 4282, B. Aboba et al., Diciembre de 2005, disponibles en línea en http://www.ietf.org/rfc/rfc4282.txt.

Otro posible identificador, que puede ser usado cuando la *CoA* es del tipo *IPv6* es la parte de la dirección *IPv6* denominada *Interface Identifer* (o *Interface ID)* (Identificador de Interfaz), que suelen ser los últimos 64 bits de los 128 bits que forman las direcciones *IPv6*. Sin embargo, no es obligatorio que una *Interface ID* tenga una longitud de 64 bits y el protocolo *IPv6* contempla que esto pueda variar en el futuro. Esta *Interface ID* es un identificador único del Nodo Móvil ya que esta parte de la dirección *CoA* no varía cuando el Nodo Móvil cambia su dirección *CoA* al cambiar de un enrutador a otro. Esto sucede, por ejemplo, si el Nodo Móvil configura su dirección IP utilizando el protocolo "*IPv6 Stateless Address Autoconfiguration*" descrito en las especificaciones *RFC* 4862, S. Thomson, et. al. Septiembre de 2007, actualmente disponible en línea en http://www.ietf.org/rfc/rfc4862.txt.

Otros identificadores son también posibles. El campo "*ID Type*" se usa para determinar qué tipo de identificador está usando el Nodo Móvil y puede tomar por ejemplo los siguientes valores:

Tipo de ID	Tipo de identificador
1	Home Address de tipo IPv4
2	Home Address de tipo IPv6
3	Network Access Identifier (NAI)
4	Interface ID

El campo "*Care-of-Address 1*" de la Figura 8 muestra qué dirección *CoA1* usó el enrutador cuando previamente se conectó al enrutador *PAR*.

El campo "*Care-of-Address 2*" muestra la nueva dirección *CoA2* que el Nodo Móvi lestá usando para enviar paquetes IP desde el enrutador NAR.

Los siguientes campos: "*Auth. Type*", "*Lenght*", "*SPI*" y "*Authenticator*" son tipos de autentificaciones que utiliza la *MSA1* y que protegen la parte del paquete *IP* 700 mostrada en la línea 770 (es decir, el paquete *IP* original antes del encapsulado).

Las Figuras 7 y 8 son ejemplos de cómo puede el Nodo Móvil enviar paquetes *IP* durante el Tiempo de Autorización Provisional incluyendo un identificador en los paquetes *IP* y autentificando la información que envía usando la *MSA1*.

Sin embargo existen otras posibilidades para que el Nodo Móvil envíe paquetes *IP* durante el Tiempo de Autorización Provisional. Una posibilidad incluye añadir identificadores del Nodo Móvil a los paquetes *IP* y autentificar los paquetes *IP* usando la *MSA1* sin incluir un bloque de datos como el *Latency Inhibition Extension* previamente descrito. Incluir un identificador del Nodo Móvil en los paquetes IP permite al *Home Agent* o al *Correspondent Node* detectar qué Nodo Móvil está enviando el paquete.

Si el identificador que está siendo usado es el *Interface ID* anteriormente definido, no es necesario añadir esta información al paquete *IP*, porque esta información ya está en el campo "*Source Address*" de la cabecera *IP* de origen para todos los paquetes *IP* que envía el Nodo Móvil desde cualquier enrutador.

Para autentificar los paquetes *IP* utilizando la *MSA1* durante el Tiempo de Autorización Provisional, el Nodo Móvil puede utilizar cualquier protocolo de autentificación, como el protocolo "*IP Authentication Header*" descrito en las especificaciones *RFC 4302*, S. Kent, Diciembre de 2005, actualmente disponible en línea en http://www.ietf.org/rfc/rfc4302.txt. Otro protocolo de autentificación especialmente adecuado para ser utilizado por el Nodo Móvil es el protocolo "*Authentication protocol for Mobile IPv6*" descrito en las especificaciones *RFC* 4285 previamente mencionadas.

En algunos nodos de red, los paquetes IP que envía un nodo de la red pueden ser modificados por algún equipo intermedio de la red. Por ejemplo, esto sucede en el protocolo titulado "Tradicional IP Network Address Translator" descrito en las especificaciones *RFC* 3022, P. Srisuresh et. al. , Enero de 2001, actualmente disponibles en línea en www.ietf.org/rfc/rfc3022.txt.

En este caso, cuando el *Home Agent* recibe el paquete *IP* modificado no puede validar la autentificación porque la firma electrónica se calculó basándose en los elementos 730 y 740 del paquete *IP* original.

Para solucionar el problema resultante de las modificaciones realizadas en el paquete *IP*, el campo "*Flags*" de la Figura 8 puede ser utilizado para incluir información que se refiere o identifica los campos modificados. Por ejemplo, un uso del campo "*Flags*" puede ser indicar que el paquete *IP* original compuesto por los elementos 730 y 740 (línea 770 de la Figura 7) puede ser modificado por la red de datos, por ejemplo por el enrutador 630, y puede haber sido modificado cuando llega al *Home Agent*.

De esta forma, el Nodo Móvil puede usar el campo "*Flags*" del bloque de datos *Latency Inhibition Extension* 720 para

indicar al *Home Agent* qué campos del paquete *IP* serán modificados y autentificar los elementos 730 y 740 mediante la adición de un valor fijo (por ejemplo, cero) en todos los bytes del campo del paquete *IP* que será modificado.

Por ejemplo, se supone que el campo que va a ser modificado es la dirección *IP* de origen del paquete *IP* original. Dicho campo se encuentra dentro de la cabecera "*Inner IP Header*" 730 de la Figura 7. Si el Nodo Móvil sabe que el campo puede ser modificado, puede calcular entonces el valor de autentificación o de firma electrónica como si el valor de dicho campo fuera una cadena de ceros, además de indicar que se ha calculado la firma electrónica mediante la adición de un "1" en el primer bit del campo "*Flags*" moviéndose de izquierda a derecha (es decir, el primer bit inmediatamente posterior al campo "*ID Type*").

Cuando el *Home Agent* recibe el paquete IP detecta que la dirección *IP* de origen del paquete ha sido modificada debido a que el primer indicador (*flag)* es, por ejemplo, un 1. Entonces, cuando comprueba la autentificación del paquete *IP*, completa los cálculos y sustituye la dirección de origen del paquete *IP* por una cadena de ceros. De esta forma el *Home Agent* puede confirmar que el paquete *IP* proviene del Nodo Móvil aunque la dirección *IP* de origen del paquete *IP* haya sido modificada en el enrutador 630.

De la misma forma, utilizando otros indicadores, el Nodo Móvil puede indicar al *Home Agent* que otros campos del paquete *IP* pueden ser modificados antes de llegar al *Home Agent* y el *Home Agent* puede confirmar la autentificación del paquete *IP* aunque dichos campos hayan sido modificados.

En otra realización, la presente invención también puede funcionar prescindiendo del proceso de Petición de Registro *(IPv4)* (*Registration Request)* y la *Binding Update (IPv6)* ya que la información enviada en estos mensajes (la nueva dirección *CoA2*, la identificación y autentificación del Nodo Móvil), ya se ha incluido en los paquetes *IP* enviados durante el Tiempo de Autorización Provisional, por ejemplo, utilizando el bloque de datos "*Latency Inhibition Extension*".

En una realización ejemplar, el *Home Agent* puede realizar un proceso de registro "implícito" mediante el análisis de los paquetes IP enviados por el Nodo Móvil durante el Tiempo de Autorización Provisional en vez de realizar un proceso de registro "explícito" utilizando los mensajes *Registration Request (IPv4)* y *Binding Update (IPv6)*. El Nodo Móvil puede confirmar que el proceso de registro "implícito" se ha realizado con éxito cuando empieza a recibir paquetes *IP* procedentes del *Home Agent* dirigidos a la nueva dirección *CoA2* que fue registrada "implícitamente". Esto también evita los mensajes *Registration Replies (IPv4)* y *Binding Acknowledgement*.

El Nodo Móvil también puede realizar un proceso de registro "implícito" en el *Correspondent Node* de forma similar a la explicada en el párrafo anterior para el *Home Agent*.

De esta forma, el proceso de registro de la nueva dirección *CoA2* se realiza automáticamente y el Nodo Móvil puede dejar de enviar la "*Latency Inhibition Extension*" tan pronto como tiene constancia de que el *Home Agent* ha completado el registro automático, ya que recibe un paquete *IP* dirigido a la nueva dirección *CoA2*. Cuando esto sucede el Nodo Móvil finaliza el Tiempo de Autorización Provisional.

Sin embargo hay que tener también en cuenta que los mensajes *Registration Request* y *Binding Update* comprenden un campo denominado "*Lifetime*" que limita el número de segundos durante los cuales el proceso de registro es válido. Este problema puede ser solucionado, por ejemplo, añadiendo un campo "*Lifetime*" al bloque de datos *Latency Inhibition Extension* descrito en la Figura 8 y reenviando periódicamente paquetes *IP* que contienen la *Latency Inhibition Extension*.

En la Figura 1, los elementos 111, 121, 131, 141 y 142 identifican las interfaces de red del *Home Agent* 110, PAR 120, NAR 130 y enrutador 140, respectivamente. Los elementos 122 y 132 se refieren a la línea de comunicación entre las antenas 122 y 123 y los enrutadores 120 y 130 respectivamente. En la Figura 2, los elementos 211, 212, 213, 214, 215, 220, 221, 222, 223, 230, 231, 232, 233, 241 y 242 corresponden a los elementos 111, 112, 113, 114, 115, 120, 121, 122, 123, 130, 131, 132, 133, 141 y 142 de la Figura 1, respectivamente. De la misma forma, en la Figura 6 los elementos 611, 612, 613, 614, 615, 620, 621, 622, 623, 630, 631, 632, 633, 641 and 642 corresponden a los elementos 111, 112, 113, 114, 115, 120, 121, 122, 123, 130, 131, 132, 133, 141 y 142 de la Figura 1, respectivamente.

REIVINDICACIONES

1. Procedimiento para la transmisión de paquetes utilizando una versión del protocolo IP Móvil Pv4 o IPV6 entre un nodo móvil y un primer nodo en una red de datos después que el nodo móvil haya transmitido paquetes de datos al primer nodo a través de un primer enrutador desde una dirección inicial *care-of-address CoA* o *co-located care-of-address CCoA* y mediante una primera asociación de seguridad con la H, un primer nodo asociado con la primera CoA o CCoA, comprendiendo el procedimiento:

el nodo móvil envía al primer nodo a través de un segundo enrutador usando una segunda dirección CoA o CCoA paquetes de datos que incluyen un identificador del nodo móvil que permite al primer nodo identificar al nodo móvil como el transmisor de los paquetes de datos durante un período de tiempo inicial después que la transmisión de los paquetes de datos a través del segundo enrutador haya comenzado; y

el nodo móvil autentifica, durante el período de tiempo inicial, los paquetes de datos que transmite al primer nodo utilizando la primera asociación de seguridad con el primer nodo asociado con la primera CoA o CCoA.

2. El procedimiento según la reivindicación 1, que comprende además: el nodo móvil simultáneamente registra con el primer nodo la segunda dirección CoA o CCoA durante el período de tiempo inicial.

3. El procedimiento según la reivindicación 1, que comprende además: el nodo móvil simultáneamente obtiene una nueva asociación de seguridad con el primer nodo durante el período de tiempo inicial.

4. El procedimiento según la reivindicación 1, que comprende además: el nodo móvil simultáneamente registra con el primer nodo la segunda dirección CoA o CCoA y obtiene una nueva asociación de seguridad con el primer nodo durante el período de tiempo inicial.

5. El procedimiento según la reivindicación 1, en el que el primer nodo es un *Home Agent* del nodo móvil.

6. El procedimiento según la reivindicación 1, en el que el primer nodo es un *Correspondent Node* del nodo móvil.

7. El procedimiento según la reivindicación 1, en el que el identificador del nodo móvil es la *Home Address* del nodo móvil.

8. El procedimiento según la reivindicación 1, en el que el identificador del nodo móvil es un Identificador de Acceso a la Red del nodo móvil.

9. El procedimiento según la reivindicación 1, en el que el identificador del nodo móvil es la parte del Identificador de Interfaz de una dirección IP del nodo móvil.

10. El procedimiento según la reivindicación 1, en el que la primera asociación de seguridad es una Asociación de Seguridad de Movilidad.

11. El procedimiento según la reivindicación 1, en el que la primera asociación de seguridad incluye el uso de una *Binding Management Key*.

12. El procedimiento según la reivindicación 1, que comprende además el uso de un protocolo de autentificación que trabaja en la capa de enlace de datos o de nivel 2 para permitir al nodo móvil acceder al segundo enrutador antes de que la segunda dirección CoA o CCoA sea autentificada con el segundo enrutador.

13. El procedimiento según la reivindicación 12, en el que el protocolo de autentificación es una versión del Protocolo de Autentificación Extensible.

14. El procedimiento según la reivindicación 2, que comprende además: el primer nodo finaliza la transmisión de paquetes de datos al nodo móvil si el registro de la segunda dirección CoA o CCoA no se ha completado dentro del período de tiempo inicial.

15. El procedimiento según la reivindicación 14, que comprende además: el primer nodo reinicia la transmisión de paquetes de datos al nodo móvil cuando el registro de la segunda dirección CoA o CCoA se ha completado.

16. El procedimiento según la reivindicación 1, en el que los paquetes de datos enviados por el nodo móvil a través del segundo enrutador están encapsulados en paquetes IP que tienen la misma dirección IP de destino igual que el primer nodo.

17. El procedimiento según la reivindicación 2, que comprende además: el primer nodo establece una asociación entre la segunda dirección CoA o CCoA y el identificador del nodo móvil; y almacena la asociación en una memoria del primer nodo.

18. El procedimiento según la reivindicación 17, que comprende además:

el primer nodo envía paquetes de datos a la segunda dirección CoA o CCoA del nodo móvil después de que se haya establecido una relación entre la segunda dirección CoA o CCoA y el identificador del nodo móvil.

19. El procedimiento según la reivindicación 16, en el que el primer nodo es un *Home Agent* y en el que el *Home Agent* elimina el encapsulado del paquete IP y reenvía los paquetes IP sin el encapsulado a un destino final del paquete.

20. El procedimiento según la reivindicación 1, en el que los paquetes de datos enviados por el nodo móvil incluyen un primer campo de datos que indica que un segundo campo de datos en el paquete de datos es modificable después de haber sido enviado por el nodo móvil, y en el que el nodo móvil autentifica los paquetes de datos como si el valor del segundo campo de datos fuera una cadena de ceros.

21. El procedimiento según la reivindicación 20, que comprende además: el primer nodo recibe los paquetes de datos y determina, basándose en el primer campo de datos, que el segundo campo de datos puede haber sido modificado; y como respuesta, el primer nodo autentifica los paquetes de datos como si el valor del segundo campo de datos fuera una cadena de ceros.

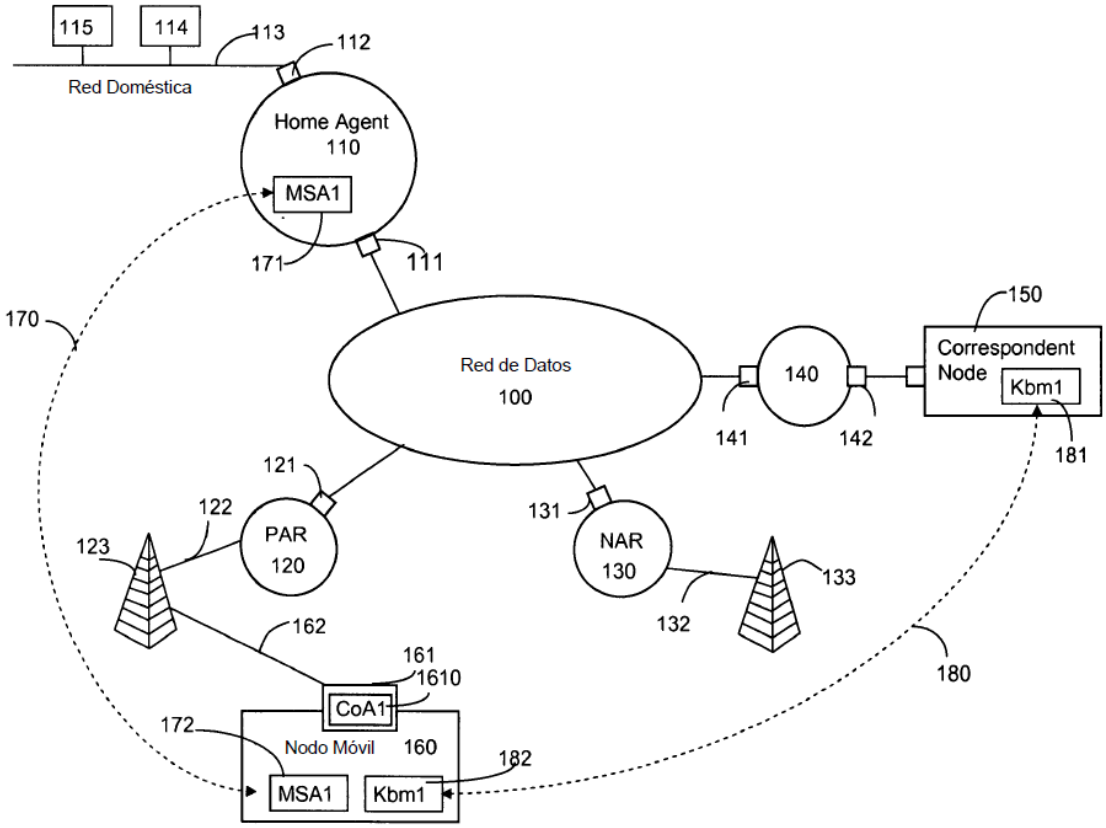
115
114
113
112
Red Doméstica
Home Agent
110
MSA1
171
111
170
Red de Datos
100
140
150
Correspondent
Node
Kbm1
141
142
181
121
122
PAR
120
131
NAR
130
123
133
132
162
161
1610
CoA1
180
172
Nodo Móvil
160
182
MSA1
Kbm1

Fig. 1

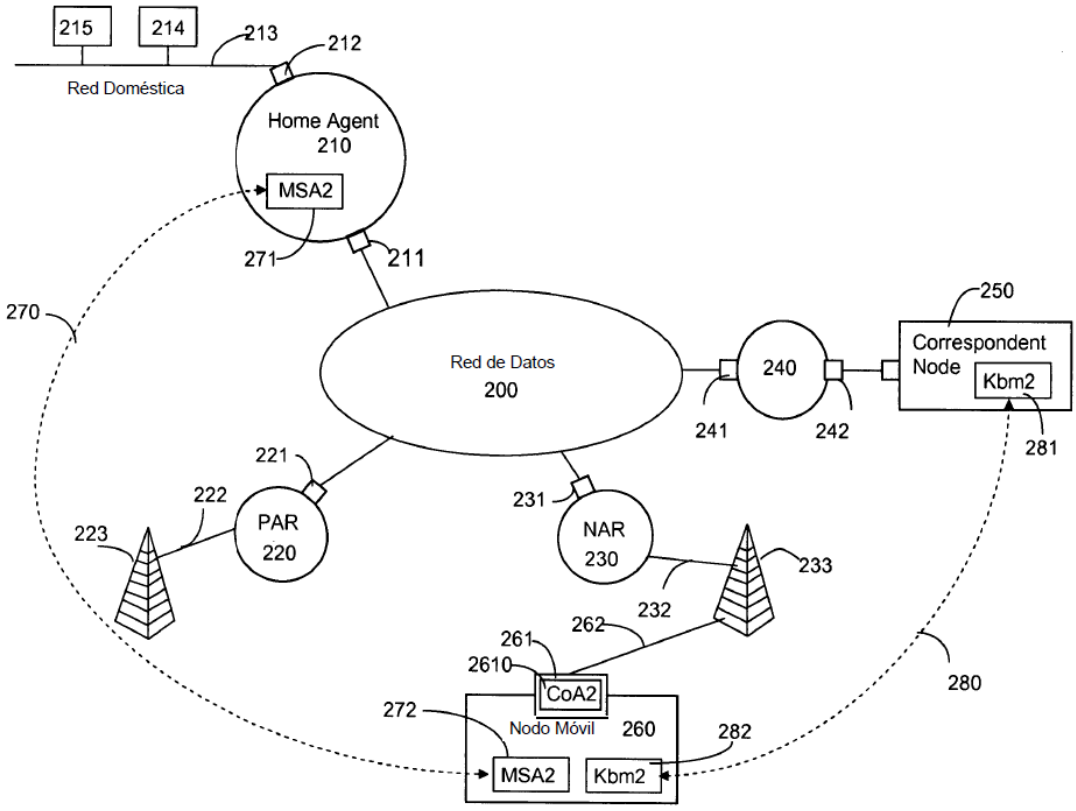
215
214
213
212
Red Doméstica
Home Agent
210
MSA2
271
211
270
Red de Datos
200
240
250
Correspondent
Node
Kbm2
241
242
281
221
222
PAR
220
231
NAR
230
223
233
232
262
261
2610
CoA2
280
272
Nodo Móvil
260
282
MSA2
Kbm2

Fig. 2

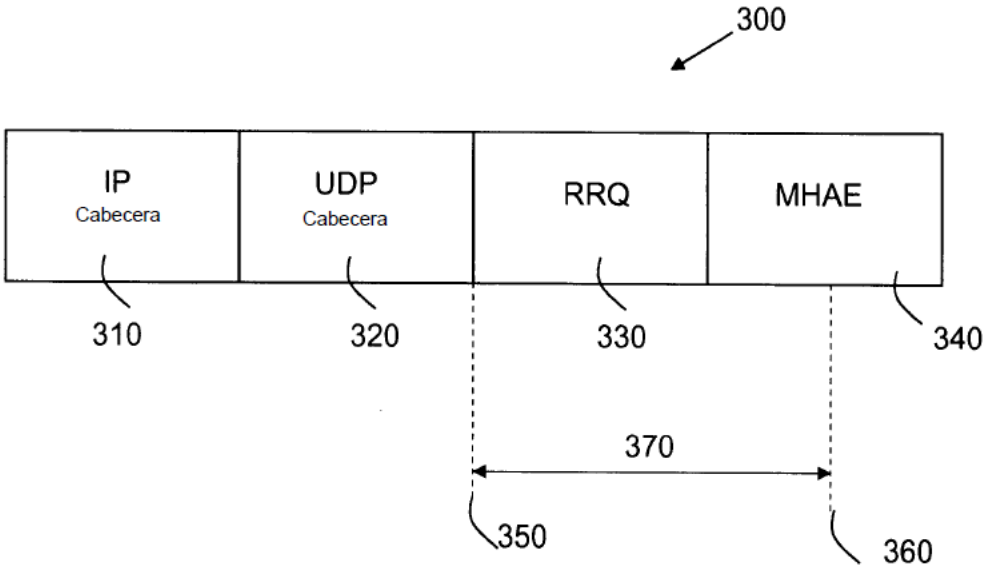
300
IP
Cabecera
UDP
Cabecera
RRQ
MHAE
310
320
330
340
370
350
360

FIG. 3

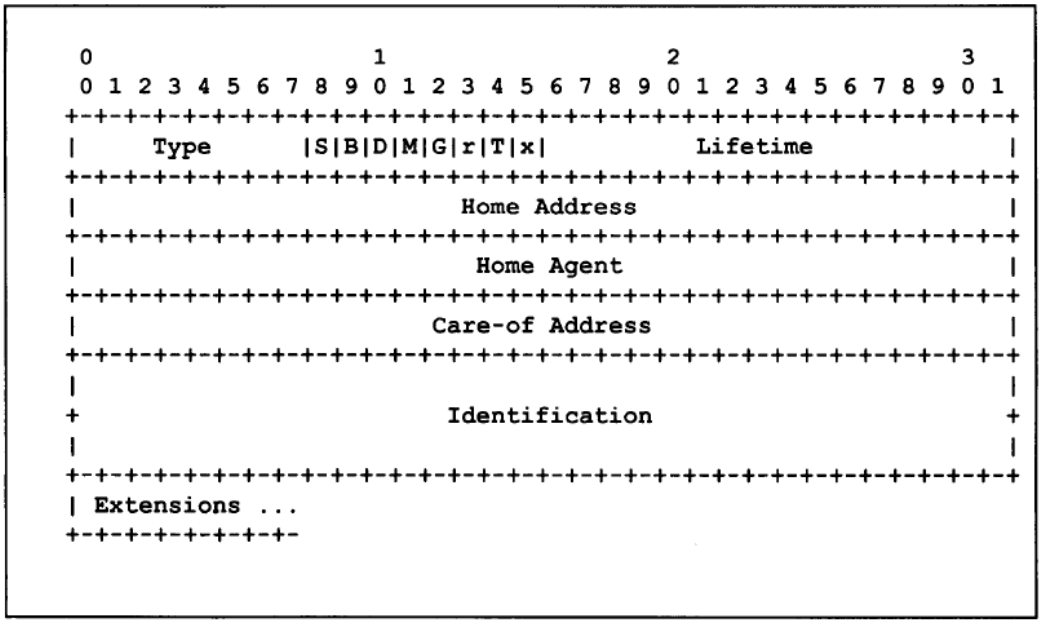
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
S B D M G r T x
Lifetime
Home Address
Home Agent
Care-of Address
Identification
Extensions ...

FIG. 4

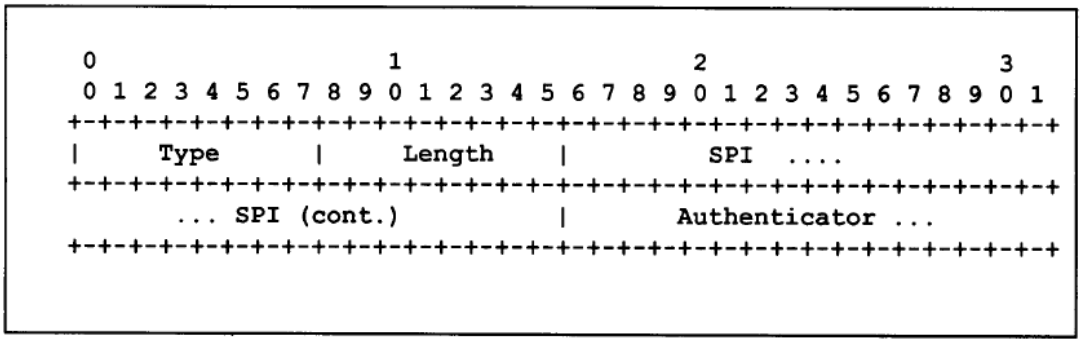
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
SPI ....
... SPI (cont.)
Authenticator ...

FIG. 5

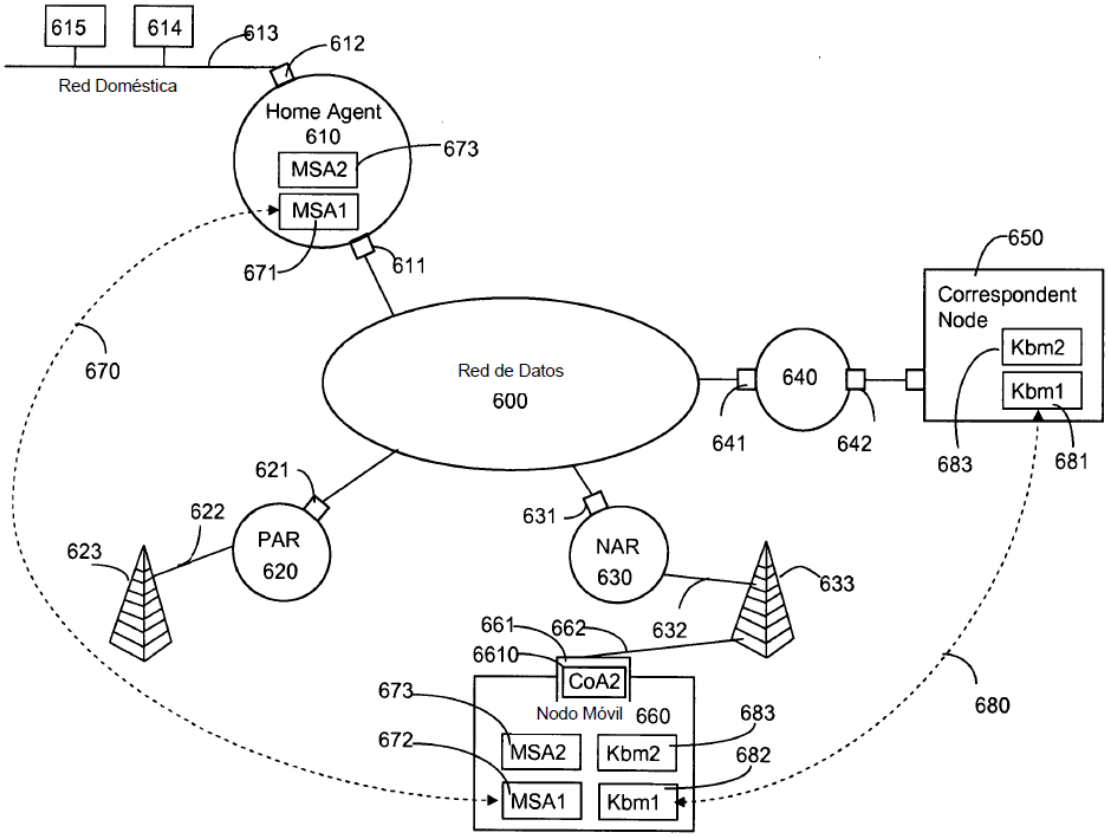
615
614
613
612
Red Doméstica
Home Agent
610
673
MSA2
MSA1
671
611
650
Correspondent
Node
Kbm2
Kbm1
670
Red de Datos
600
640
641
642
683
681
621
622
623
PAR
620
631
NAR
630
633
661
662
632
6610
CoA2
673
Nodo Móvil
660
683
672
MSA2
Kbm2
682
MSA1
Kbm1
680

Fig. 6

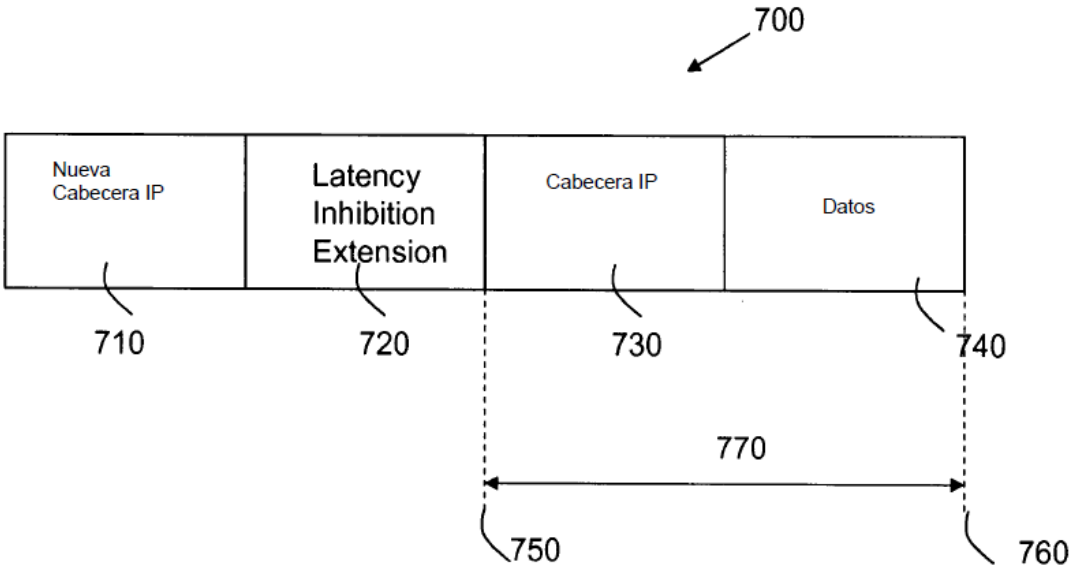
700
Nueva Cabecera IP
Latency Inhibition Extension
Cabecera IP
Datos
710
720
730
740
770
750
760

FIG. 7

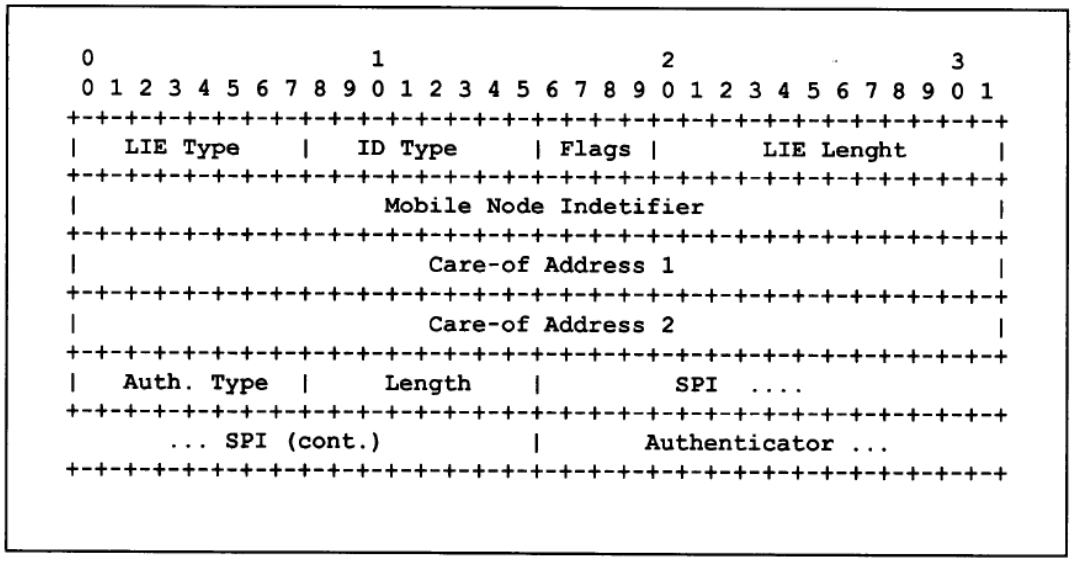
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
LIE Type
ID Type
Flags
LIE Lenght
Mobile Node Indetifier
Care-of Address 1
Care-of Address 2
Auth. Type
Length
SPI ....
... SPI (cont.)
Authenticator ...

FIG. 8

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patentes citados en la descripción

US 20070177550 A1

Literatura diferente de patentes citadas en la descripción

• IP Mobility Support for IPv4'' protocol (hereafter, ''Mobile IPv4. **C. PERKINS.** RFC 3344 specifications) IETF, August 2002

• **D. JOHNSON et al.** RFC 3775 specifications. IETF, June 2004

• **PERKINS et al.** RFC. ed online by the IETF, October 2003

• **G. MONTENEGRO.** RFC 3024, January 2001, http://www.ietf.org/rfc/rfc3024.txt

• Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. **J. ARKKO et al.** security mechanisms first recommended by the IEFT for use in Mobile lPv6. IETF, June 2004

• **S. KENT et al.** RFC 4301 specifications. IETF, December 2005

• Authentication Protocol for Mobile IPv6. **A. PATEL et al.** RFC 4285 specifications. IEFT, January 2006

• Mobile IPv6 Operation with IKEv2 and the revised IPsec architecture. **V. DEVARAPALLI et al.** RFC 4877. IETF, April 2007

• **C. RIGNEY et al.** RFC 2865 specifications. IETF, June 2000

• **C. PERKINS et al.** RFC 3957 specifications. IETF, March 2005

• Fast Handover for Mobile IPv6. **R. KOODLI.** RFC 4068 specifications. IETF, July 2005

Hierarchical Mobile IPv6 Mobility Management. **H. SOLIMAN et al.** RFC 4140 specifications. IETF, August 2005

• **D. MAUGHAN et al.** RFC 2408 specifications. IETF, November 1998

• Authentication, Authorization and Accounting (AAA) Registration Keys for Mobile IPv4. **C. PERKINS et al.** RFC 3957. March 2005

• **B. ABOBA et al.** RFC 3748 specifications, June 2004, http://www.ietf.org/rfc/rfc3748.txt

• **HESHAM SOLIMAN.** Mobile IPv6 support for dual stack Host and Routers, November 2007, http://tools.ietf.org/html/draft-ietf-mip6-nemo-v4traversal-06

• **B. ABOBA et al.** RFC 4282 specifications, December 2005, ilable online at http://www.ietf.org/rfc/rfc4282.txt

• **S. THOMSON et al.** RFC 4862 specifications, September 2007, http://www.ietf.org/rfc/rfc4862.txt.

• **S. KENT.** RFC 4302 specifications, December 2005, http://www.ietf.org/rfc/ric4302.txt

• **P. SRISURESH et al.** Traditional IP Network Address Translator. RFC 3022 specifications, January 2001, www.ietf.org/rfc/rfc3022.txt