(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 449 574**

(51) Int. CI.:

H04W 8/06 (2009.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 8/12 (2009.01)
H04W 80/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.09.2007 E 07820435 (1)**

(97) Fecha y número de publicación de la concesión europea: **15.01.2014 EP 2210429**

(54) Título: **Método y aparato para itinerancia entre redes de comunicaciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.03.2014

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm , SE

(72) Inventor/es:

SUGIMOTO, SHINTA;
ODA, TOSHIKANE y
KATO, RYOJI

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y aparato para itinerancia entre redes de comunicaciones

Campo técnico

La invención se refiere al campo de la itinerancia entre redes de comunicaciones.

Antecedentes

El IP para móviles (MIP), que ha sido descrita en IETF RFC 3344, permite a los usuarios de dispositivos para comunicaciones móviles moverse desde una red a otra mientras mantienen una dirección de IP permanente, con independencia de la red en la que se encuentren. Esto permite al usuario mantener conexiones mientras se está desplazando. Por ejemplo, si un usuario estuviera participando en una sesión de Voz sobre IP (VoIP) y el usuario se moviera durante la sesión de una red a otra, sin soporte de MIP podría cambiar la dirección de IP del usuario. Esto podría conducir a problemas con la sesión de VoIP.

Un Nodo Móvil (MN) está asignado a dos direcciones de IP: una dirección local permanente y una dirección de custodia (CoA). La CoA está asociada a un nodo de la red que el usuario visita normalmente. Para comunicar con el MN, se envían paquetes a la dirección local de MN. Estos paquetes son interceptados por un Agente Local en la red local, que tiene conocimiento de la CoA actual. El Agente Local tuneliza después los paquetes hasta la CoA del MN con una nueva cabecera de IP, mientras que conserva la cabecera de IP original. Cuando los paquetes son recibidos por el MN, éste retira la nueva cabecera de IP y obtiene la cabecera de IP original. El MN envía paquetes directamente a otro nodo a través de un agente extraño de la red visitada. El agente extraño conserva información acerca de los MNs visitantes, incluyendo la CoA de cada MN visitante.

Proxy Mobile IP v6 (MIPv6), IETF draft-sgundave-mip6-proxymip6-01, describe una función de Agente Proxy Móvil (PMA). Esta función emula propiedades de enlace local con el fin de hacer que un MN se comporte como si éste estuviera en su red local y permita soportar movilidad por las redes que de otro modo no podría soportar MIPv6.

Se implementa normalmente un PMA en el enrutador de acceso. El PMA envía y recibe señales relacionadas con la movilidad en representación de un MN. Cuando un MN conecta con un enrutador de acceso que tiene un PMA, el MN presenta su identidad en forma de Identificador de Acceso de Red (NAI) como parte de un procedimiento de autenticación de acceso. Una vez que el MN ha sido autenticado, el PMA obtiene el perfil de usuario a partir de un almacén de directivas. El PMA, que tiene conocimiento del perfil de usuario y del NAI, puede ahora emular la red local del MN. El MN obtiene a continuación su dirección local desde el PMA. El PMA informa también al Agente Local del MN sobre la posición actual del MN usando un mensaje de Actualización de Enlace. El mensaje de Actualización de Enlace utiliza el NAI del MN. Tras la recepción del mensaje de Actualización de Enlace, el Agente Local configura un túnel hasta el PMA y envía un reconocimiento de enlace al PMA. Con la recepción del Reconocimiento de Enlace, el PMA configura un túnel hasta el Agente Local. Todo el tráfico procedente del MN es enrutado hasta el Agente Local a través del túnel.

El Agente Local recibe cualquier paquete que sea enviado al MN, y reenvía el paquete recibido hasta el PMA a través del túnel. Con la recepción del paquete, el PMA retira la cabecera de túnel y envía el paquete al MN. El PMA actúa como enrutador por defecto sobre el enlace de acceso. Cualesquiera paquetes que sean enviados desde el MN son enviados a través del PMA hasta el Agente Local, el cual envía después el paquete hasta el destino final.

Resulta posible que un MN deambule desde un dominio Proxy MIP a otro. En el ejemplo ilustrado en la Figura 1, un MN deambula desde un dominio Proxy MIP Local hasta un dominio Proxy MIP visitado. Para asegurar continuidad para cualquiera de las sesiones en las que el MN esté actualmente participando, el MN sigue usando su Agente Local (HAh) en vez del Agente Local (HAv) del dominio Proxy MIP Visitado, incluso aunque el PMA que da servicio al MN esté en el dominio visitado. En ese caso, el PMA que da servicio al MN es PMA1v una vez que el MN se ha desplazado al dominio Visitado.

Según la especificación PMIPv6 actual, a efectos de que ocurra itinerancia, se establece un túnel (ilustrado en la Figura 1 mediante una línea de puntos) entre el Agente Local HAh y el PMA (en este caso, PMA1v) que da servicio al MN en el dominio visitado. Con el fin de establecer un túnel, se requiere una relación de confianza entre HAh y PMA1v. Ocurre un problema en el escenario de itinerancia, debido a que HAh y PMA1v pertenecen a dominios Proxy MIP diferentes. Es posible establecer una relación de confianza entre HAh y PMA1v. Sin embargo, esto conduce a problemas de escalabilidad, ya que esto podría requerir que todos los Has de todos los dominios Proxy MIP tengan una relación de confianza con todos los PMAs de todos los dominios Proxy MIP con anterioridad a cualquier itinerancia, lo que no es práctico.

Otro problema de itinerancia entre dominios Proxy MIP se presenta cuando el dominio Proxy MIP Local está en una red cerrada. Una red cerrada puede estar, por ejemplo, protegida mediante un cortafuegos. Esta situación ha sido ilustrada en la Figura 2. En ese caso, establecer un túnel entre HAh y PMA1v resulta imposible a menos que el cortafuegos entre las dos redes reconozca que PMA1v goza de la confianza de HAh. El cortafuegos podría necesitar por lo tanto tener conocimiento de todas las relaciones de confianza entre Has y PMAs de todos los dominios Proxy

MIP.

H. Ohnishi et al., “Mobile IPv6 AAA Problem statement draft-ohnishi-mip6-aaa-problem-statement-00.txt” IETF [Online], Febrero de 2004, describe que no se establece el procedimiento de AAA para un Nodo Móvil que deambule por una red visitada y que la solución aplicada a IPv4 no puede ser utilizada. S. Gundavelli et al., “Proxy Mobile Ipv6-draft-sgundave-mip6-proxymip6-02.txt” IETF [Online], 5 de Marzo de 2007, describe una solución de protocolo para gestión de movilidad basada en red, pero no describe ninguna forma de seleccionar una puerta de enlace. M Ghassemian et al., “Análisis de direccionamiento y alternativas QoS para conectividad ad hoc con Internet”, Comunicaciones de radio Personales, Interiores y Móviles, 2003. PIMRC 2003.14 IEEE Proceedings del 7-10 de Septiembre de 2003, describe el principio de aplicar puertas de enlace de internet para el acceso de nodos móviles a Internet a través de redes de acceso fijas, pero no se enfoca sobre IP de Móviles y se refiere a un nodo que selecciona una puerta de enlace sobre la base de QoS. P. Calhoun et al., “RFC 4004: Aplicación Diametro Móvil IPv4” IEFT [Online], Agosto de 2005 describe un procedimiento de AAA usando el protocolo DIAMETRO en una red IPv4 Móvil.

Sumario

Los inventores han resuelto los problemas asociados al establecimiento de relaciones de confianza entre nodos de red en dominios diferentes, y han diseñado aparatos y métodos para reducir esos problemas.

Según un primer aspecto de la invención, se proporciona un método de gestionar itinerancia de un Nodo Móvil en una red Visitada. El nodo móvil está asociado a una red Local. Un servidor de Autenticación, Autorización y Contabilización (AAA) dispuesto en la red Visitada, selecciona un nodo de Puerta de Enlace dispuesto entre la red Local y la red Visitada para su uso por el Nodo Móvil. La selección se basa en criterios de selección. Una vez que se ha seleccionado el nodo de Puerta de Enlace, el servidor envía un mensaje a un nodo de acceso de la red Visitada a la que está sujeto el Nodo Móvil, cuyo mensaje identifica el nodo de Puerta de Enlace seleccionado. Una ventaja del método cuando se utiliza en una red Proxy-MIP consiste en que no hay necesidad de que un Agente Proxy Móvil establezca una relación de confianza con Agentes Locales de otras redes. El método permite también que un Nodo Móvil mantenga asociación segura con su Red Local, incluso cuando el Nodo Móvil es itinerante en una red Visitada cerrada. El método puede ser usado también para seleccionar un Punto de Anclaje Móvil para su uso por parte de un Nodo Móvil en una red MIPv6 Jerárquica.

Usando un servidor de AAA, se puede hacer programación previa del nodo de Puerta de Enlace como parte de un procedimiento de autenticación normal.

En caso de que la invención sea implementada en una red Proxy-MIP, el nodo de Puerta de Enlace es un nodo de Puerta de Enlace de IP de Proxy Móvil, y el nodo de acceso es un Agente Proxy Móvil.

La invención comprende opcionalmente, con anterioridad a la selección de un nodo de Puerta de Enlace, recibir un mensaje de autorización desde un servidor de Autenticación, Autorización y Contabilización dispuesto en la red Local. El mensaje de autorización comprende un identificador que identifica un Agente Local en la red Local. El identificador se encarga de identificar el nodo de Puerta de Enlace seleccionado, y el mensaje de autorización con el identificador cambiado se envía al nodo de acceso.

Se pueden usar cualesquiera criterios de selección adecuados para seleccionar el nodo de Puerta de Enlace. Éstos incluyen opcionalmente cualquiera de una apuesta de confianza entre el nodo de Puerta de Enlace y la red Local, y la distancia entre el nodo de acceso y el nodo de Puerta de Enlace.

Mientras las funciones de un nodo de Puerta de Enlace son implementadas opcionalmente en un compartimento simple, las funciones del nodo de Puerta de Enlace están distribuidas opcionalmente entre la red Local y la red Visitada. En este caso, los criterios de selección comprenden la selección de funciones individuales. Si es este el caso y el nodo de Puerta de Enlace es un nodo de Puerta de Enlace de IP de Proxy Móvil, entonces las funciones pueden incluir una función de emulación de Agente Local y una función de Agente Proxy Móvil.

En el caso de una red de IP Móvil Jerárquica, el nodo de Puerta de Enlace es opcionalmente un Punto de Anclaje de Movilidad y el nodo de acceso es un Enrutador de Acceso.

Según una segunda realización de la invención, se proporciona un servidor de Autenticación, Autorización y Contabilización para su uso en una red Visitada de una red de comunicación. El servidor comprende medios para seleccionar un nodo de Puerta de Enlace dispuesto entre una red Local y una red Visitada en base a criterios de selección, y un transmisor para enviar un mensaje a un nodo de acceso de la red Visitada, cuyo mensaje identifica el nodo de Puerta de Enlace seleccionado.

En una red Proxy MIP, el servidor comprende además opcionalmente un receptor para recibir un mensaje de autorización desde un servidor de Autenticación, Autorización y Contabilización dispuesto en la red Local, comprendiendo el mensaje de autorización un identificador que identifica un Agente Local de la red Local. Se proporcionan medios para cambiar el identificador que identifica el nodo de Puerta de Enlace seleccionado, y así el mensaje enviado al nodo de acceso es el mensaje de autorización con el identificador cambiado.

En el caso de una red de IP Móvil Jerárquica, el servidor comprende opcionalmente un receptor para recibir un mensaje de autorización desde un servidor de Autenticación, Autorización y Contabilización Local, dispuesto en la red Local. El servidor comprende además medios para seleccionar un Punto de Anclaje de Movilidad para su uso por un Nodo Móvil sujeto a la red atendida por el servidor de Autenticación, Autorización y Contabilización, y medios para añadir un Par de Valor - Atributo que identifique al Punto de Anclaje de Movilidad respecto al mensaje de autorización con anterioridad a su transmisión hasta el nodo de acceso de la red Visitada. De esta manera, un Nodo Móvil puede ser dotado de un Punto de Anclaje de Movilidad durante el proceso de autenticación.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente un diagrama de bloques de una itinerancia de Nodo Móvil desde un dominio Proxy MIP Local hasta un dominio Proxy MIP visitado;

La Figura 2 ilustra esquemáticamente, en un diagrama de bloques, una itinerancia de un Nodo Móvil desde un dominio Proxy MIP Local hasta un dominio Proxy MIP visitado, donde el dominio Proxy MIP Local está protegido por un cortafuegos;

La Figura 3 ilustra esquemáticamente la arquitectura de una red Proxy MIP Local y una red Proxy MIP visitada, disponiendo de una Puerta de Enlace Proxy MIP dispuesta en una interfaz entre las dos redes Proxy MIP;

La Figura 4 ilustra esquemáticamente, en un diagrama de bloques, la asignación dinámica de una Puerta de Enlace de Proxy MIP a un Nodo Móvil itinerante;

La Figura 5 es un diagrama de flujo que ilustra las etapas para seleccionar una Puerta de Enlace de proxy MIP según una realización de la invención;

La Figura 6 ilustra esquemáticamente, en un diagrama de bloques, un servidor de Autenticación, Autorización y Contabilización según una realización de la invención;

La Figura 7 es un diagrama de flujo de señal que muestra las señales entre los nodos ilustrados en la Figura 4;

La Figura 8 ilustra esquemáticamente la arquitectura de una red Proxy MIP Local y una red Proxy MIP Visitada, que tiene una Puerta de Enlace Proxy MIP dispuesta en una interfaz entre las dos redes Proxy MIP, según una realización de la invención en la que están distribuidas algunas funciones de la Red de Enlace de Proxy MIP, y

La Figura 9 ilustra esquemáticamente la arquitectura de una red Proxy MIP Local y un dominio Móvil Jerárquico Visitado IPv6 según una realización adicional de la invención.

Descripción detallada

Haciendo referencia a la Figura 3, se introduce una Puerta de Enlace Proxy MIP en una interfaz entre un dominio Proxy MIP Local y un dominio Proxy MIP Visitado. La Puerta de Enlace Proxy MIP emula tanto un Agente Local (HA) que es local en un dominio, y un Agente Proxy Móvil (PMA) que es local en el otro dominio. Con el fin de implementar una Puerta de Enlace Proxy MIP, los propietarios de las dos redes deben estar de acuerdo con situar una Puerta de Enlace Proxy MIP en el borde entre las redes. La puerta de Enlace Proxy MIP pertenece tanto al dominio Proxy MIP Local como al dominio Proxy MIP Visitado. Esto puede ser implementado como un único compartimento físico o puede ser implementado a modo de funciones distribuidas a través de cada red.

En el ejemplo de la Figura 3, cuando el Nodo Móvil (MN) ha itinerado desde el dominio Local hasta el dominio Visitado, la Puerta de Enlace Proxy MIP se comporta como un PMA en el dominio Proxy MIP Local y como un HA para el dominio Proxy MIP Visitado. El PMA debe proporcionar por lo tanto las mismas interferencias para el HA en el dominio Proxy MIP Local que proporcionan PMA1h y PMA2h, y de forma similar debe proporcionar las mismas interferencias en el dominio Visitado que las proporcionadas por un Agente Local (HAv) a los PMAs en la red Visitada.

Todo el tráfico enviado al, o desde el, MN itinerante en el dominio Proxy MIP Visitado, atraviesa la Puerta de Enlace Proxy MIP. Según atraviesa el tráfico la Puerta de Enlace Proxy MIP, un cortafuegos puede discernir en el dominio Local el tráfico procedente del MN itinerante respecto a otro tráfico, y por lo tanto sabe que no necesita aplicar las políticas de cortafuegos normales que podrían ser aplicadas al tráfico de IP normal que no llegue desde una fuente de confianza. A efectos de hacer esto, el cortafuegos necesita solamente confiar en las Puertas de Enlace de PMA en el interior de la red Local, en vez de en todas las de los PMAs de todas las redes Proxy MIP.

Cuando un MN está deambulando por una red Visitada, es necesario seleccionar la Puerta de en Enlace Proxy MIP más relevante para su uso por el MN itinerante. El aprovisionamiento de la Puerta de Enlace Proxy MIP puede hacerse estáticamente, pero es extremadamente ineficiente y el recurso es intensivo. Es por lo tanto mejor que el aprovisionamiento de la Puerta de Enlace de PMAIP se realice dinámicamente.

Haciendo referencia a la Figura 4, se ha ilustrado esquemáticamente la asignación dinámica de una Puerta de Enlace Proxy MIP a un Nodo Móvil itinerante. En este ejemplo, existen tres dominios Proxy MIP, un dominio Proxy

MIP Local, un dominio Proxy MIP Visitado, y Otro dominio Proxy MIP. Se han ilustrado también tres Puertas de Enlace Proxy MIP. La PMIP-GW1 y la PMIP-GW2 pertenecen tanto al dominio Proxy MIP Local como al dominio Proxy MIP Visitado, y la PMIP-GW3 pertenece tanto al dominio Proxy MIP Visitado como al Otro dominio Proxy MIP.

Si un MN deambula por el dominio Proxy MIP Visitado, es importante que se seleccione PMIP-GW1 o PMIP-GW2, puesto que estas Puertas de Enlace Proxy MIP tienen una relación de confianza con el Agente Local HAh en el dominio Proxy MIP Local, mientras que PMIP-GW3 no tiene esa relación de confianza. De forma similar, PMIP-GW1 y PMIP-GW2 no podrán ser seleccionadas para ninguno de los Nodos Móviles que deambulan desde el Otro dominio Proxy MIP hasta el dominio Visitado, debido a que PMIP-GW1 y PMIP-GW2 no tienen ninguna relación de confianza con el Agente Local HAo en el Otro dominio Proxy MIP.

Con el fin de seleccionar una Puerta de Enlace Proxy MIP adecuada para un MN, se utiliza un servidor proxy de Autenticación, Autorización y Contabilización (AAA) en la red visitada en la que el MN está deambulando. Los servidores de AAA son entidades que proporcionan funcionalidad de IP para soportar las funciones de Autenticación, Autorización y Contabilización. Los servidores de AAA están especificados en el protocolo RADIUS (véase C. Rigney, S. Willens, A. Rubens, W. Simpson, “Marcación de Aute4nticación Remota En Servicio de Usuario (RADIUS)”, IETF RFC2865, 2000-06) y el protocolo DIAMETRO (véase P. Calhoun, J. Lougnhney, E. Guttman, G. Zorn, J. Arkko, “Protocolo de Base Diametro”, IETF RFC3588, 2003-09). Los servidores de AAA residen tanto en el dominio Proxy MIP Local como en el dominio Proxy MIP Visitado. El servidor de AAA (AAAh) del dominio Proxy MIP Local funciona como un servidor de autenticación, y el servidor AAA (AAAv) del dominio Proxy MIP Visitado funciona como un servidor proxy.

La especificación PMIPv6 especifica que el servidor AAAh de AAA autoriza el HA de PMIPv6 del PMA (y el Prefijo de Red Local y la Dirección Local) dentro de una sesión de AAA. En la etapa 1 de la Figura 4, el AAAh envía un mensaje Diametro al AAAv con una indicación de que HAh es el agente local PMIPv6 para el MN. El AAAv, en su capacidad como servidor proxy de AAA, selecciona 2 una Puerta de Enlace Proxy MIP (en este caso, la PMIP-GW1) en base a un conjunto específico de criterios y a continuación informa 3 al PMA (en este caso, el PMA1v) de la Puerta de Enlace Proxy MIP seleccionada.

Los criterios de selección usados por AAAv deben incluir la selección de una Puerta de Enlace Proxy MIP que pertenece al dominio Proxy MIP Local del MN, por ejemplo la posición geográfica de la Puerta de Enlace Proxy MIP, el equilibrio de carga en la red, o cualquier otro criterio decidido por el operador de red.

En el ejemplo de la Figura 4, cualquiera de entre PMIP-GW1 o PMIP-GW2 podría ser seleccionada para el MN, puesto que ambas gozan de la confianza del HAh. La PMIP-GW1 se selecciona por lo tanto en base a otros criterios, por ejemplo debido a que PMIP-GW1 sea topológicamente más cercana a PMA1v que PMIP-GW2.

Según se muestra en la Figura 4, AAAv cambia el valor del indicador de Agente Local PMIPv6 en el mensaje Diametro respecto al PMA1v desde el “HAh” hasta la “PMIP-GW1”. En base a la información que identifica la Puerta de Enlace Proxy MIP seleccionada, proporcionada por este mecanismo, PMA1v envía una Actualización de Enlace Proxy (BU) a PMIP-GW1, y a continuación PMIP-GW1 envía la BU Proxy a HAh.

El servidor proxy de AAA no tiene necesidad de seleccionar una Puerta de Enlace Proxy MIP si el HA PMIPv6 y el PMA tienen una relación de confianza y establecen un túnel entre ellos. En esos casos, el servidor de AAA del dominio Proxy MIP Visitado actúa como servidor de retransmisión de AAA, y no como servidor proxy de AAA. En ese caso, éste enrutará los mensajes a otros nodos de AAA, sin modificar los mensajes de AAA.

Se puede decir que el servidor proxy de AAA (AAAv) “programa previamente” la Puerta de Enlace Proxy MIP en el interior del dominio visitado durante el procedimiento de autenticación de extremo a extremo del MN con su servidor de AAA local (AAAh). La programación previa es un procedimiento destinado a provisionar la puerta de enlace de modo que pueda ofrecer servicios al MN autenticado. Obsérvese que en tecnologías convencionales, AAAh juega el papel principal en la programación previa de las entidades de red incluyendo las presentes en el dominio de red visitado.

El servidor proxy de AAA (AAAv) notifica también al autenticador de AAA el perfil de la puerta de enlace seleccionada. Puesto que el AAAv toma la decisión de la selección de puerta de enlace, es necesario que el autenticador de AAA tenga conocimiento de la puerta de enlace seleccionada con el fin de llevar a cabo el control de acceso y mantener materiales de generación de clave para un MN dado.

Las etapas básicas para seleccionar una Puerta de Enlace Proxy MIP, han sido ilustradas en la Figura 5. En la etapa 501, como parte de un procedimiento de autorización normal cuando un MN deambula por una red Visitada, el AAAh envía un mensaje de autorización al AAAv. El mensaje identifica el Agente Local en la red local, HAh. El AAAv selecciona 502 qué Puerta de Enlace Proxy MIP debe ser usada por el Nodo Móvil, y cambia 503 el identificador en el mensaje procedente del HAh a un identificador que identifique la Puerta de Enlace Proxy MIP seleccionada. A continuación se envía 504 el mensaje a un PMA al que esté unido el MN.

Haciendo referencia a la Figura 6, se han ilustrado los componentes básicos requeridos por el AAAv. El AAAv 601 comprende un receptor 602 para recibir el mensaje procedente del AAAh, y un procesador 603 para seleccionar una

Puerta de Enlace Proxy MIP, y un procesador 603 para seleccionar una Puerta de Enlace Proxy MIP. La selección puede requerir el uso de información procedente de una base de datos 604, la cual puede estar o no dispuesta en el AAAv. El procesador 603 se usa también para alterar la identidad en el mensaje procedente del HAh respecto a la de la Puerta de Enlace Proxy MIP seleccionada. El AAAv 601 comprende además un transmisor 605 para enviar el mensaje a un PMA al que está unido el MN.

Haciendo referencia a la Figura 7, se ha mostrado un diagrama de flujo de señal que muestra las señales entre los nodos ilustrados en la Figura 4.

El MN tiene una cuenta con el dominio Proxy MIP Local, y un identificador tal como User@Home.Net. “Home.Net” representa la red del dominio Proxy MIP Local en este ejemplo. El protocolo de AAA de aplicaciones para usuario (entre el MN y un PMA) es 802.1x, y el protocolo de AAA de servicios de fondo (entre un PMA y un servidor de AAA) es Diametro. Por supuesto, se pueden usar otros protocolos, por ejemplo, PPP, PANA, o IKEv2 en vez de 802.1x, y Radius en vez de Diametro. Se supone que los PMAs en el dominio Proxy MIP Visitado reenvían los mensajes de Diametro-Petición al servidor de AAA local (AAAv).

La secuencia de generación de señales es como sigue, con referencia a la numeración de la Figura 5.

701) Cuando el MN se desplaza al dominio Proxy MIP Visitado, el MN envía 4 un mensaje 802.1x a PMA1v como petición de autenticación. Se especifica User@Home.Net como identificador en el paquete 802.1x.

702) Cuando se recibe el paquete 802.1x procedente del MN, PMA1v envía un mensaje de Diametro-Petición al AAAv. La Petición incluye los datos de autenticación especificados en el paquete 802.1x recibido.

703) AAAv reenvía el mensaje de Diametro-Petición al AAAh. El AAAv obtiene la identificación del AAAh desde la parte de dominio del identificador User@Home.Net.

704) El AAAh autentica el MN.

705) Tras la autenticación con éxito, el AAAh envía un mensaje de Diametro-Éxito al AAAv. El Agente Local se establece en “HAh”, y el Prefijo de Red Local (NHP) asignado al Nodo Móvil se establece en “Pf”.

706) Tras la recepción del mensaje de Diametro-Éxito procedente del AAAh, el AAAv selecciona PMIP-GW1 como Puerta de Enlace Proxy MIP para el MN, puesto que PMIP-GW1 tiene un túnel (es decir, una relación de confianza) con HAh. El AAAv envía un mensaje de Registro-Petición a la PMIP-GW1 que incluye una indicación de que registre “HAh” como el HA para el Prefijo de Red local “Pf”. El protocolo para transportar el Registro-Petición puede ser cualquier protocolo adecuado, por ejemplo, Diametro, COPS, SNMP.

707) Tras la recepción del mensaje de Registro-Petición desde el AAAv, la PMIP-GW1 registra “HAh” como un HA para el Prefijo de Red Local “Pf”. Este registro se utiliza más tarde en la etapa 12 con el fin de identificar “HAh” como el HA para el Prefijo de Red local “Pf”.

708) La PMIP-GW1 envía un mensaje de Registro-Respuesta al AAAv.

709) AAAv envía un mensaje de Diametro-Éxito a PMA1v. El valor del indicador de Agente Local se establece en “PMIP-GW l”.

710) PMA1v envía una Actualización de Enlace Proxy (PBU) a PMIP-GW1, que indica que el Prefijo de Red Local es “Pf” y que la Dirección de Custodia (CoA) es “PMA1v”.

711) Tras la recepción de la PBU desde PMA1v, la PMIP-GW1 crea una entrada de caché de enlace (BCE) para el Prefijo de Red Local “Pf”. La CoA de esta entrada es “PMA1v”.

712) La PMIP-GW1 envía una PBU a HAh, puesto que “HAh” está registrado como el HA para “Pf” (véase la etapa 7). La CoA de esta PBU es “PMIP-GW1”.

713) Tras la recepción de la PBU procedente de la PMIP-GW1, HAh crea una entrada caché de enlace (BCE) para el Prefijo de Red local “Pf”. La CoA de esta entrada en “PMIP-GW1”.

714) HAh envía un Reconocimiento de Enlace Proxy (PBA) a PMIP-GWI.

715) PMIP-GW1 envía un PBA a PMA1v.

716) PMA1v envía un mensaje 802.1x al MN indicando el resultado con éxito.

Después de este procedimiento, el PMA1v actúa como enrutador por defecto para el MN según se especifica en IETF draft-sgundave-mip6-proxymip6-01.

Los paquetes de enlace descendente vinculados al MN son suministrados al HAh, y a continuación reenviados a la PMIP-GW1, puesto que HAh tiene una BCE para Pf (MN) cuya CoA es PMIP-GW1. Los paquetes son reenviados a

continuación a PMA1v puesto que PMIP-GW1 tiene una BCE que indica que la CoA de Pf (MN) es PMA1v. Los paquetes son finalmente reenviados al MN.

Los paquetes de enlace ascendente procedentes del MN son suministrados as PMA1v, reenviados a continuación a PMIP-GWI, después a HAh, y finalmente reenviados a la dirección de destino.

En algunas redes, las funciones de una Puerta de Enlace pueden estar distribuidas. Este escenario ha sido ilustrado en la Figura 8. En este ejemplo, las funciones son implementadas en 5 compartimentos físicos: BOXh1, BOXh2, BOXh3, BOXh4 y BOXh5.

BOXh1 y BOXh2 actúan como funciones PMA en el Dominio Proxy MIP Local, y BOXv3, BOXv4 y BOXv5 actúan como funciones HA en el dominio Proxy MIP Visitado. Los compartimentos están enlazados entre sí para el intercambio de tráfico itinerante.

En tal distribución funcional, la selección de la Puerta de Enlace Proxy MIP consiste en:

1. Seleccionar una función PMA a partir de BOXh1 y BOXh2;

2. Seleccionar una función HA a partir de BOXv3, BOXv4 y BOXv5, y

3. Enlazar la función PMA seleccionada y la función HA seleccionada.

En el ejemplo de la Figura 8, se selecciona una función PMA a partir de BOXh1, y se selecciona una función HA a partir de BOXv5. Combinadas, éstas se comportan como una PMIP-GW.

Para tal distribución funcional, el conjunto de criterios para la selección puede resultar complicado, pero por otra parte, resulta posible una selección optimizada. Por ejemplo, seleccionando una función PMA (a partir de BOXh1 o BOXh2) que sea topológicamente más cercana a HAh, y una función HA (a partir de BOXv3, BOXv4, o BOXv5) que sea topológicamente más cercana a PMA1v, la trayectoria de enrutamiento entre el MN y el HAh puede ser optimizada, como se muestra mediante las líneas gruesas en la Figura 6.

La invención puede ser implementada también en una red Móvil Jerárquica IPv6. El concepto básico de la selección y el aprovisionamiento de una Puerta de Enlace Proxy MIP y la modificación de un mensaje de AAA por el servidor de AAA, pueden ser aplicados en MAP Discovery en HMIPv6. Aunque MAP no es una puerta de enlace de MIPv6, se pueden aplicar principios similares. La Figura 9 ilustra un ejemplo de la invención aplicado a una red HMIPv6.

Haciendo referencia a la numeración de las etapas de la Figura 9:

901) Se envía un mensaje de AAA (Diametro-Petición) desde el Enrutador de Acceso AR1 al AAAv cuando el MN accede a AR1.

902) El mensaje de AAA es reenviado desde el AAAv hasta el AAAh. Puede existir mensajería adicional entre MN y AAAh para autenticación, pero no se ha ilustrado en la Figura 7 por motivos de claridad.

903) AAAh envía un mensaje de éxito de AAA a AAAv cuando la autenticación ha tenido éxito. Cuando recibe el mensaje de éxito de AAA, el AAAv añade un Par de Valor - Atributo (AVP) de Punto de Anclaje de Movilidad (MAP) al mensaje de éxito de AAA. La selección de un MAP se basa en un conjunto específico de criterios. Por ejemplo, en la Figura 7 se elige MAP1.

904) AAAv envía el mensaje de éxito de AAA incluyendo “MAP1” como el valor AVP de MAP a AR1, puesto que el mensaje de éxito de AAA incluye el AVP de MAP.

905) AR1 envía un anuncio de enrutador IPv6 al MN. El anuncio incluye “MAP1” como el valor de la opción MAP.

Las credenciales entre el MN y MAP1 pueden ser una clave secreta compartida derivada de una Clave de Sesión Maestra (MSK) generada por el Protocolo de Autenticación Extensible (EAP). En tales casos, se necesita un protocolo de aprovisionamiento entre el AAAv y el MAP. Este protocolo puede ser similar al usado en las etapas 6 y 8 ilustradas en la Figura 5.

Si el MN accede a AR3, el AAAv puede añadir “MAP2” puesto que el valor de APV de MAP y “MAP2” pueden ser anunciados como MAP a partir de AR3 en base a un conjunto específico de criterios, por ejemplo debido a que el MAP2 está topológicamente más cerca de AR3 que MAP1.

La invención descrita en lo que antecede tiene diversas ventajas sobre la técnica anterior. Ésta reduce los costes de mantenimiento de asociaciones entre PMAs y HAs, puesto que no existe necesidad de que un PMA establezca una relación de confianza con HAs en otros dominios de red. Además, cuando un MN deambula hasta una red Local cerrada, mantiene una asociación segura con su red Local. La invención no tiene ningún impacto sobre Agentes Locales existentes, Agentes Móviles Proxy, o Nodos Móviles. Además, no existe ningún impacto sobre los protocolos usados, tal como el protocolo Proxy MIPv6 o los protocolos de AAA (por ejemplo, Radius, Diameter,

802.1x, etc.). Se pueden aplicar los mismos principios u otros similares a redes Proxy MIP (IPv4) y HMIPv6.

Los expertos en la materia podrán apreciar que se pueden realizar diversas modificaciones en las realizaciones anteriormente descritas sin apartarse del alcance de la presente invención. Por ejemplo, mientras la invención ha sido descrita usando los ejemplos de Proxy MIP o PMIPv6, se apreciará que también puede ser usada para cualquier protocolo que soporte puertas de enlace o puertas de enlace proxy.

En la descripción se han usado los siguientes acrónimos:

AAA	Autenticación, Autorización y Contabilización
AP	Punto de Acceso
AR	Enrutador de Acceso
AVP	Par de Valor-Atributo
BA	Reconocimiento de Enlace
BC	Caché de Enlace
BCE	Entrada de Caché de Enlace
BU	Actualización de Enlace
BUL	Lista de Actualización de Enlace
CoA	Dirección de Custodia
CN	Nodo Correspondiente
COPS	Protocolo de Servicio de Política Común Abierta
EAP	Protocolo de Autenticación Extensible
GW	Puerta de Enlace
HA	Agente Local
HMIPv6	MIPv6 Jerárquico
HNP	Prefijo de Red Local
HoA	Dirección Local
IP	Protocolo de Internet
IPv6	IP versión 6
LAN	Red de Área Local
MAP	Punto de Anclaje de Movilidad
MIP	IP Móvil
MIPv6	IPv6 Móvil
MN	Nodo Móvil
MSK	Clave de Sesión Maestra
NAS	Servidor de Acceso de Red
PBA	Reconocimiento de Enlace Proxy
PBU	Actualización de Enlace Proxy
PMA	Agente Proxy Móvil
PMIP	IP de Proxy Móvil
PMIPv6	IPv6 de Proxy Móvil

SNMP Protocolo de Gestión de Red Simple

W-LAN LAN inalámbrica

REIVINDICACIONES

1.- Un método de gestionar itinerancia de un Nodo Móvil en una red Visitada, estando el Nodo Móvil asociado a una red Local, estando el método **caracterizado por**:

en un servidor de Autenticación, Autorización y Contabilización dispuesto en la red Visitada, seleccionar (706) un nodo de Puerta de Enlace en base a criterios de selección, estando el nodo de Puerta de Enlace dispuesto entre la red Local y la red Visitada;

en el servidor de Autenticación Autorización y Contabilización, enviar (709) un mensaje a un nodo de acceso de la red Visitada al que está unido el Nodo Móvil, cuyo mensaje identifica el nodo de Puerta de Enlace seleccionado.

2.- El método según la reivindicación 1, en donde el nodo de Puerta de Enlace es un nodo de Puerta de Enlace de IP de Proxy Móvil, y el nodo de acceso es un Agente Proxy Móvil.

3.- El método según la reivindicación 1 ó 2, que comprende además;

con anterioridad a seleccionar un nodo de Puerta de Enlace, recibir (705) un mensaje de autorización desde un servidor de Autenticación, Autorización y Contabilización dispuesto en la red Local, comprendiendo el mensaje de autorización un identificador que identifica un Agente Local de la red Local;

cambiar el identificador para que identifique el nodo de Puerta de Enlace seleccionado, y

enviar el mensaje de autorización con el identificador cambiado al nodo de acceso.

4.- El método según una cualquiera de las reivindicaciones anteriores, en donde los criterios de selección comprenden uno cualquiera de entre una relación de confianza entre el nodo de Puerta de Enlace y la red Local, y la distancia entre el nodo de acceso y el nodo de Puerta de Enlace.

5.- El método según una cualquiera de las reivindicaciones anteriores, en donde las funciones del nodo de Puerta de Enlace están distribuidas entre la red Local y la red Visitada, y los criterios de selección comprenden la selección de funciones individuales.

6.- El método según la reivindicación 5, en donde el nodo de Puerta de Enlace es un nodo de Puerta de Enlace de IP de Proxy Móvil, y las funciones incluyen una función de emulación de Agente Local y una función de Agente Proxy Móvil.

7.- El método según la reivindicación 1, en donde el nodo de Puerta de Enlace es un Punto de Anclaje de Movilidad y el nodo de acceso es un Enrutador de Acceso.

8.- Un servidor (601) de Autenticación, Autorización y Contabilización para su uso en una red de comunicación, comprendiendo el servidor:

medios (603) para seleccionar un nodo de Puerta de Enlace, dispuesto entre una red Local y una red Visitada a la que el Nodo Móvil, MN, está unido en base a criterios de selección, y

un transmisor (605) para enviar un mensaje a un nodo de acceso de la red Visitada, cuyo mensaje identifica el nodo de Puerta de Enlace seleccionado;

en donde el servidor de Autenticación, Autorización y Contabilización está dispuesto de modo que se sitúa en la red Visitada.

9.- El servidor de Autenticación, Autorización y Contabilización según la reivindicación 8, que comprende además:

un receptor (602) para recibir un mensaje de autorización desde un servidor de Autenticación, Autorización y Contabilización dispuesto en la red Local, comprendiendo el mensaje de autorización un identificador que identifica un Agente Local en la red Local;

estando el servidor de Autenticación, Autorización y Contabilización **caracterizado por** comprender medios para cambiar el identificador para que identifique el nodo de Puerta de Enlace seleccionado;

en donde el mensaje enviado al nodo de acceso es el mensaje de autorización con el identificador cambiado.

10.- El servidor de Autenticación, Autorización y Contabilización según la reivindicación 9, que comprende además:

un receptor (602) para recibir un mensaje de autorización desde un servidor de Autenticación, Autorización y Contabilización Local, dispuesto en la red Local;

medios para seleccionar un Punto de Anclaje de Movilidad para su uso por un Nodo Móvil unido a la red atendida por el servidor de Autenticación, Autorización y Contabilización;

medios para añadir un Par de Valor - Atributo que identifica el Punto de Anclaje de Movilidad respecto al mensaje de autorización con anterioridad a la transmisión del mismo al nodo de acceso en la red Visitada.

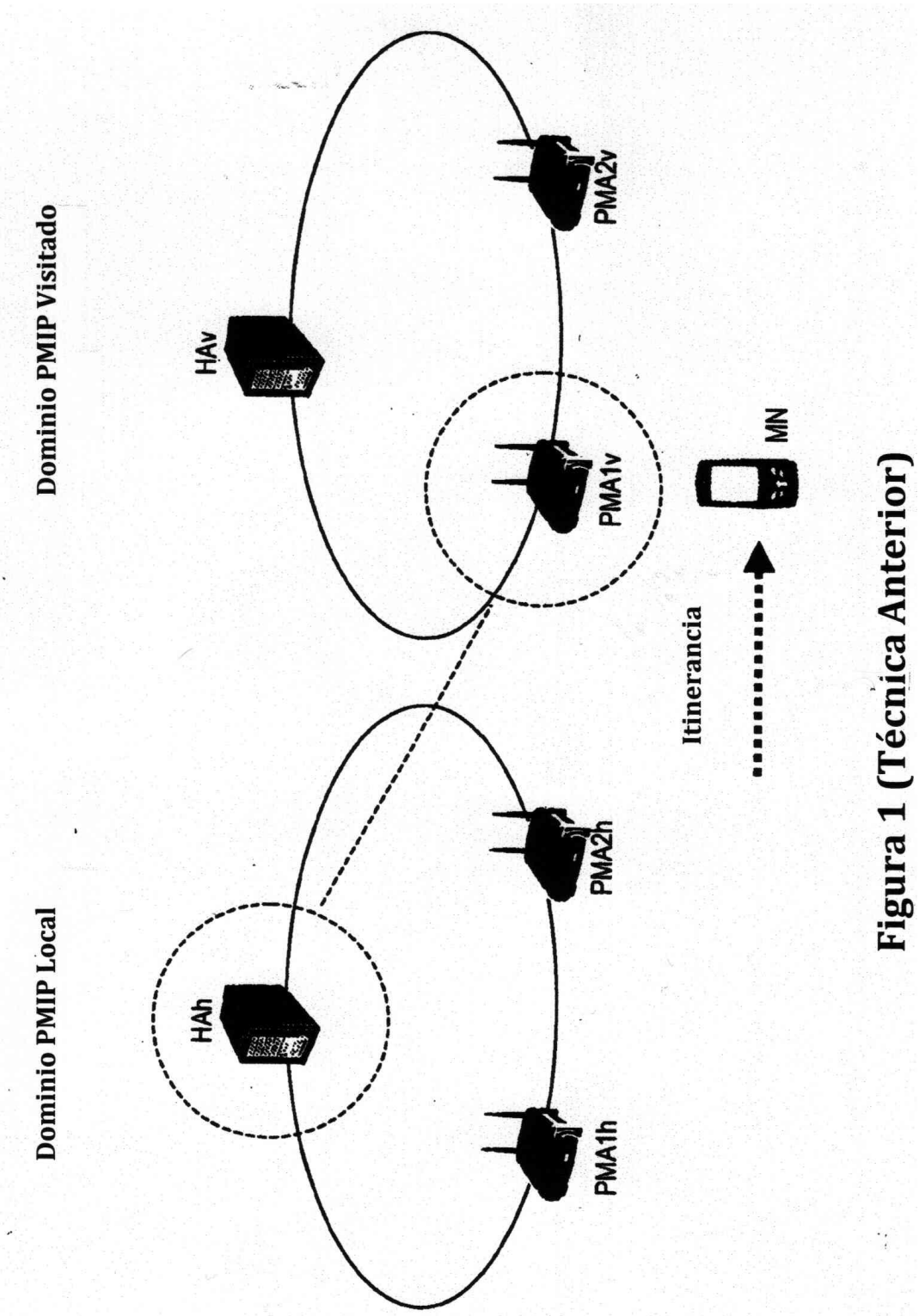

Figura 1 (Técnica Anterior)

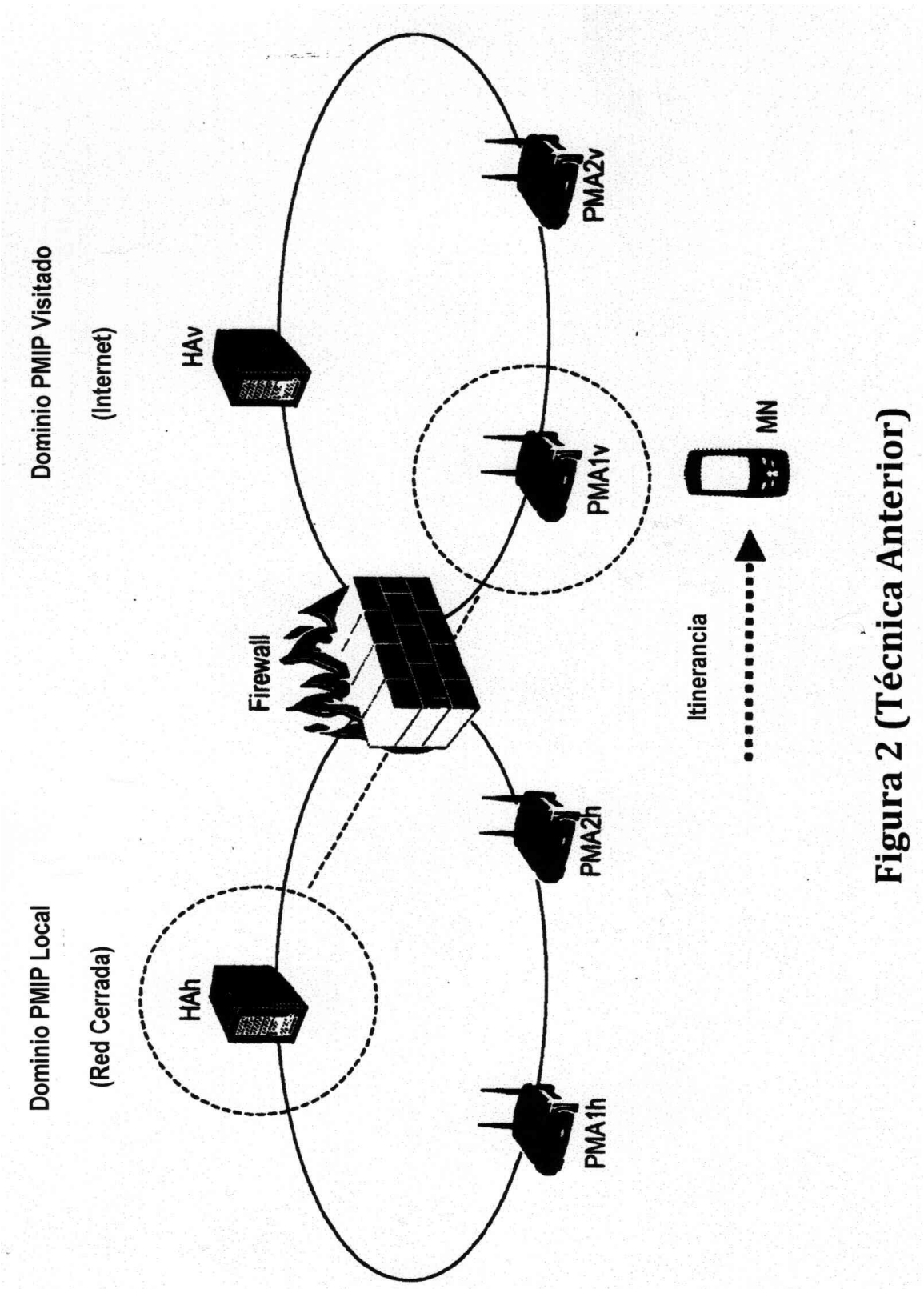

Figura 2 (Técnica Anterior)

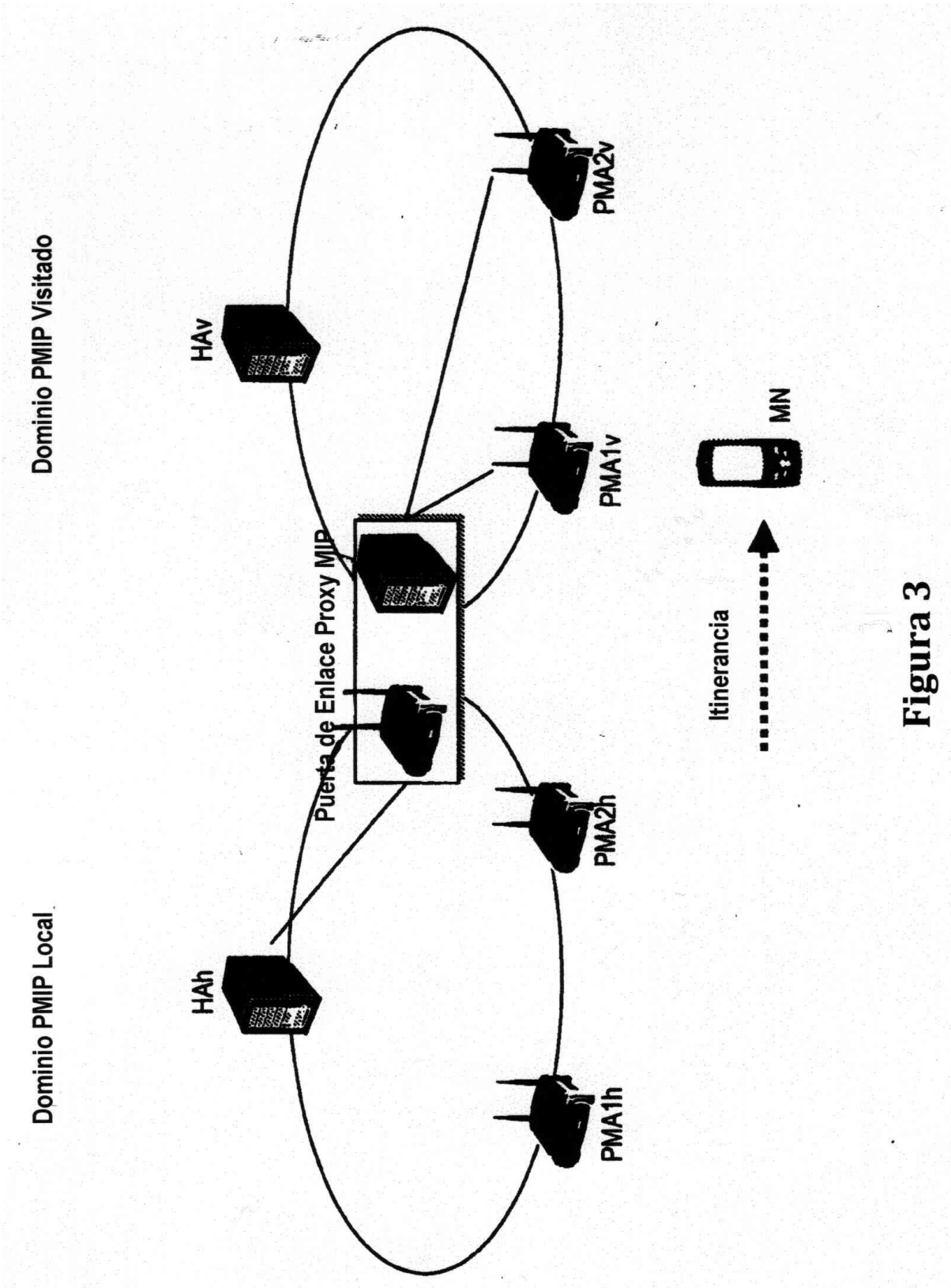
Dominio PMIP Visitado
Dominio PMIP Local
HAv
HAh
PMA2v
PMA1v
PMA2h
PMA1h
Puerta de Enlace Proxy MIP
Itinerancia
MN

Figura 3

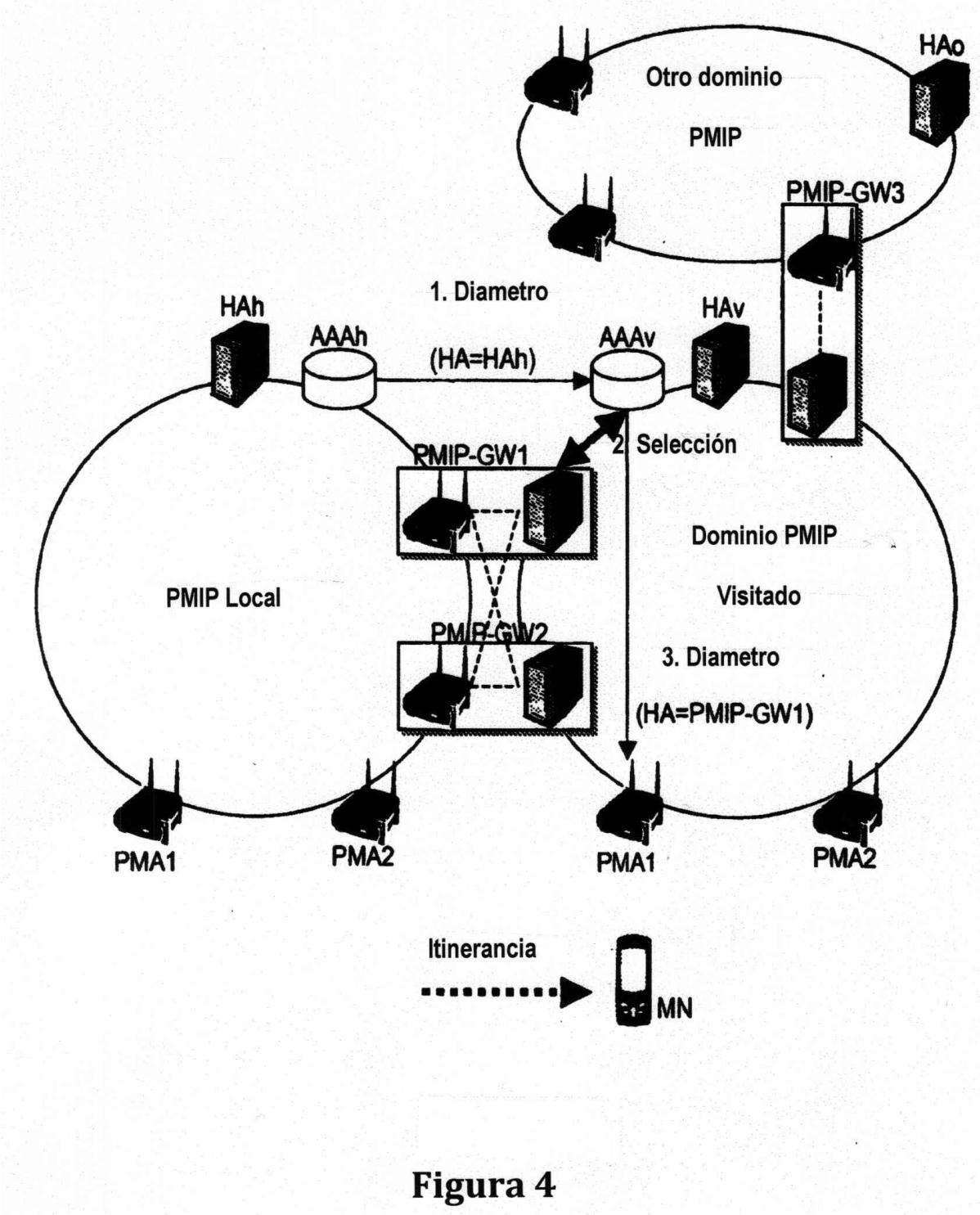
HAo
Otro dominio
PMIP
PMIP-GW3
1. Diametro
HAh
AAAh
(HA=HAh)
AAAv
HAv
2. Selección
PMIP-GW1
Dominio PMIP
PMIP Local
Visitado
PMIP-GW2
3. Diametro
(HA=PMIP-GW1)
PMA1
PMA2
PMA1
PMA2
Itinerancia
MN

Figura 4

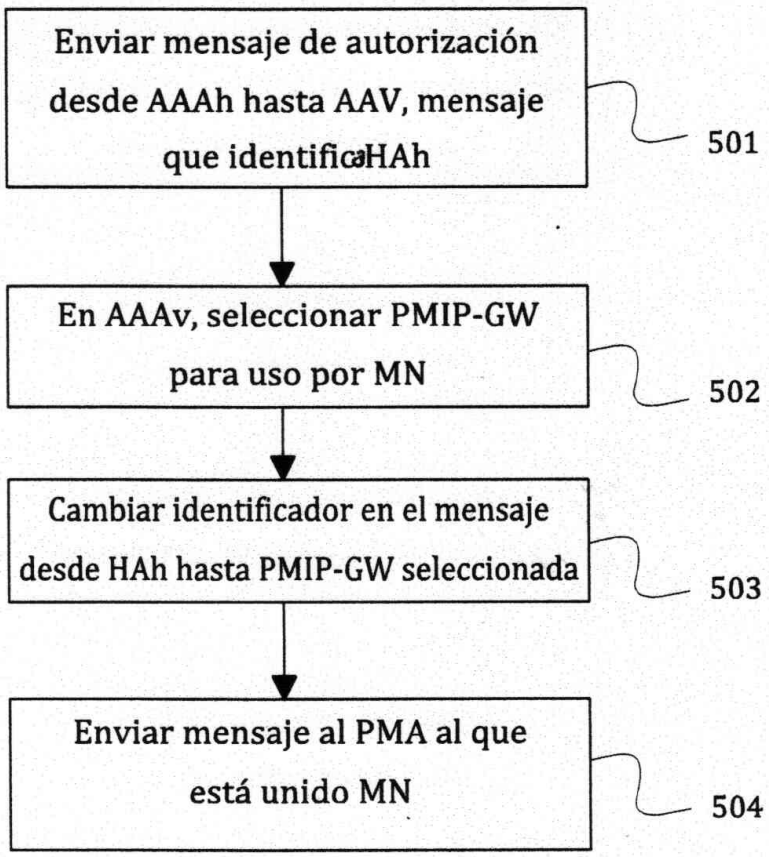

Figura 5

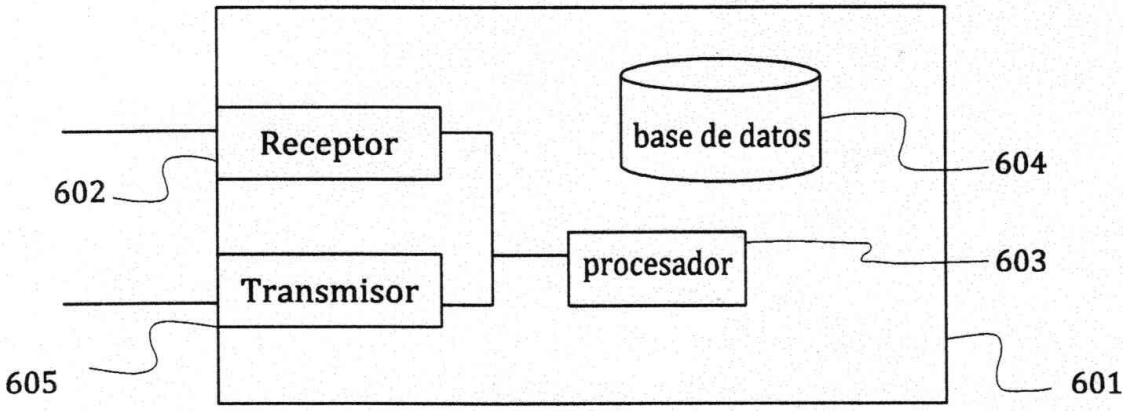

Figura 6

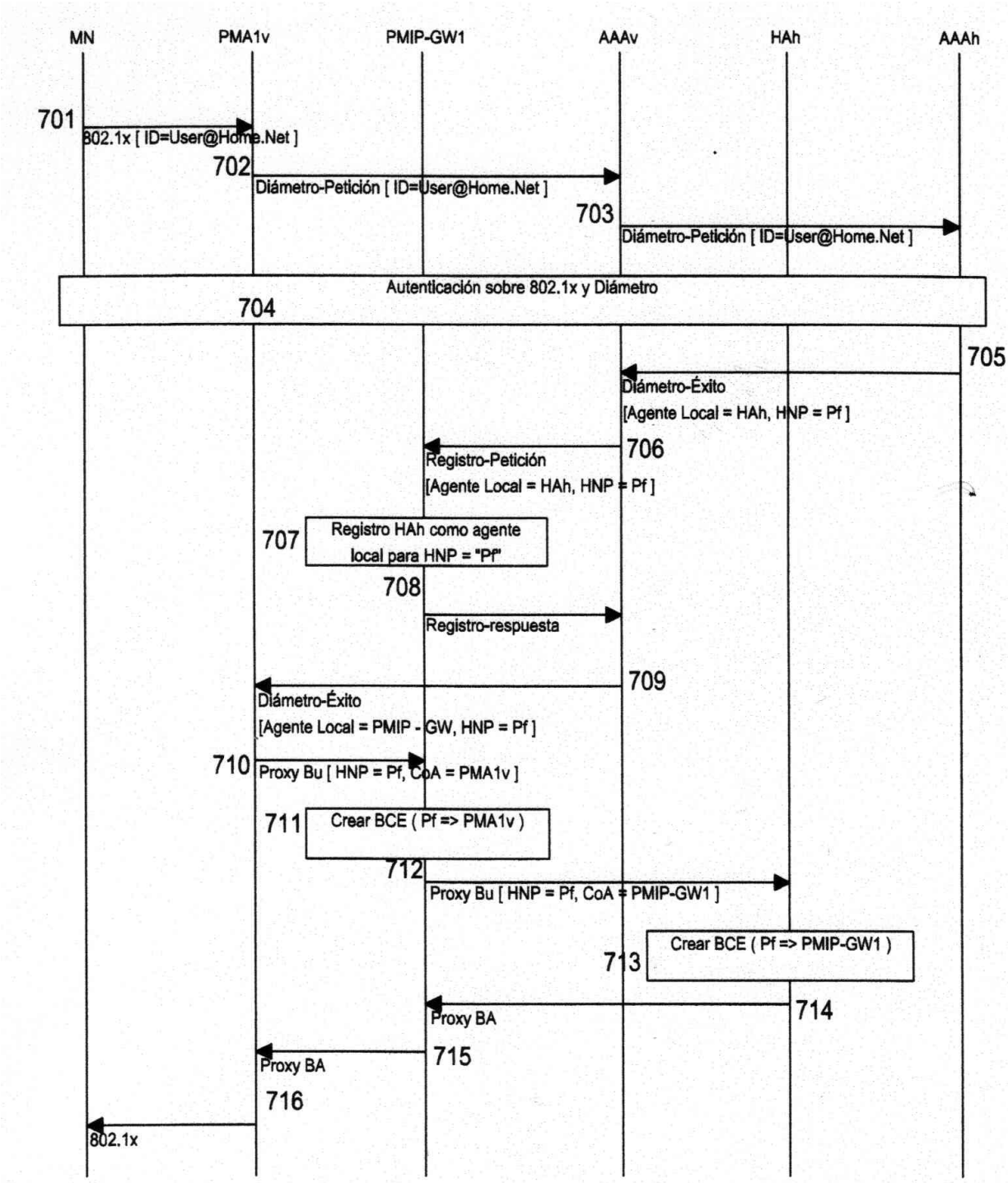
MN
PMA1v
PMIP-GW1
AAAv
HAh
AAAh
701
802.1x [ID=User@Home.Net]
702
Diámetro-Petición [ID=User@Home.Net]
703
Diámetro-Petición [ID=User@Home.Net]
Autenticación sobre 802.1x y Diámetro
704
705
Diámetro-Éxito
[Agente Local = HAh, HNP = Pf]
706
Registro-Petición
[Agente Local = HAh, HNP = Pf]
707
Registro HAh como agente local para HNP = "Pf"
708
Registro-respuesta
709
Diámetro-Éxito
[Agente Local = PMIP - GW, HNP = Pf]
710
Proxy Bu [HNP = Pf, CoA = PMA1v]
711
Crear BCE (Pf => PMA1v)
712
Proxy Bu [HNP = Pf, CoA = PMIP-GW1]
713
Crear BCE (Pf => PMIP-GW1)
714
Proxy BA
715
Proxy BA
716
802.1x

Figura 7

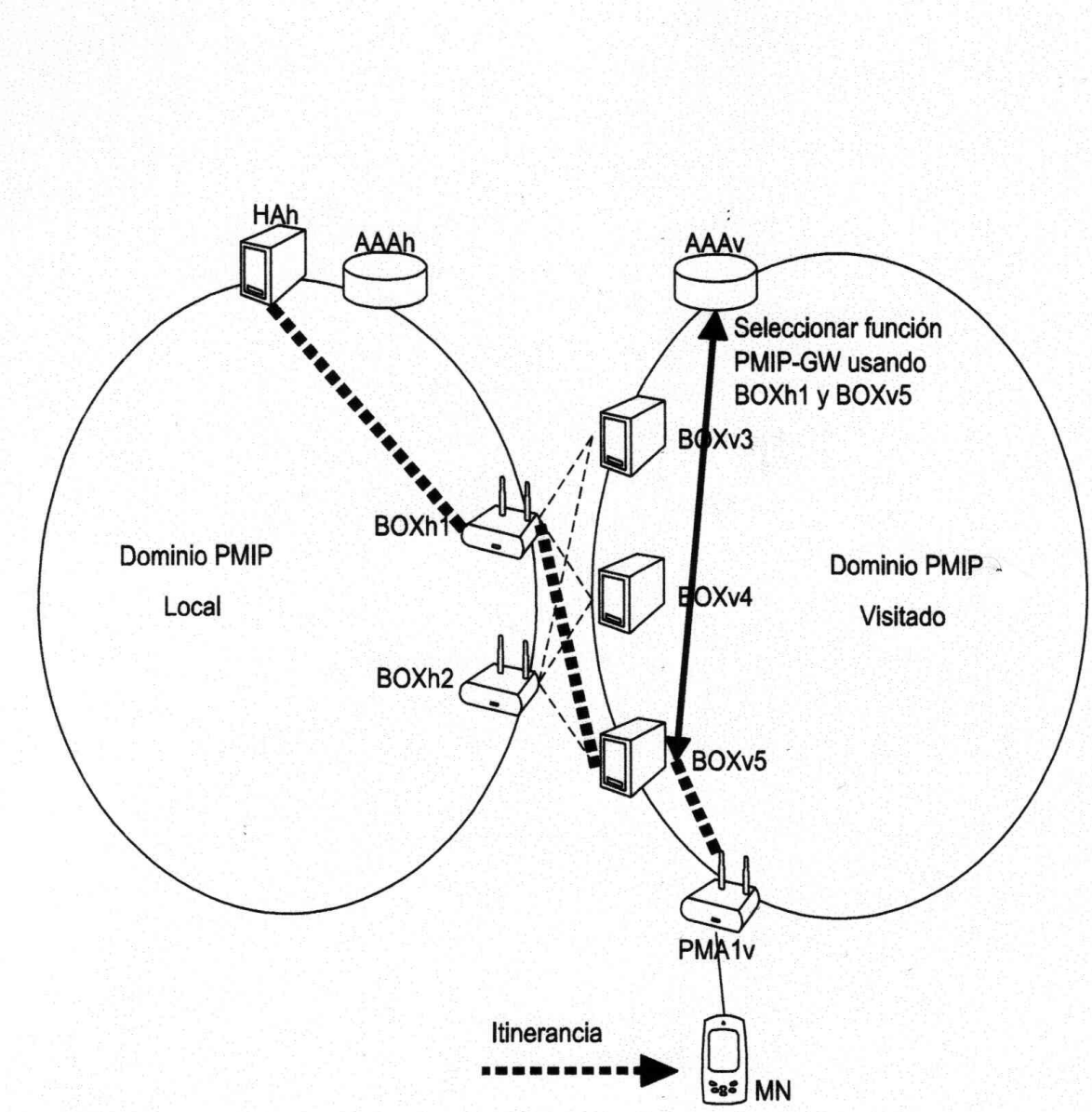
HAh
AAAh
AAAv
Seleccionar función
PMIP-GW usando
BOXh1 y BOXv5
BOXv3
BOXh1
Dominio PMIP
Local
Dominio PMIP
Visitado
BOXv4
BOXh2
BOXv5
PMA1v
Itinerancia
MN

Figura 8

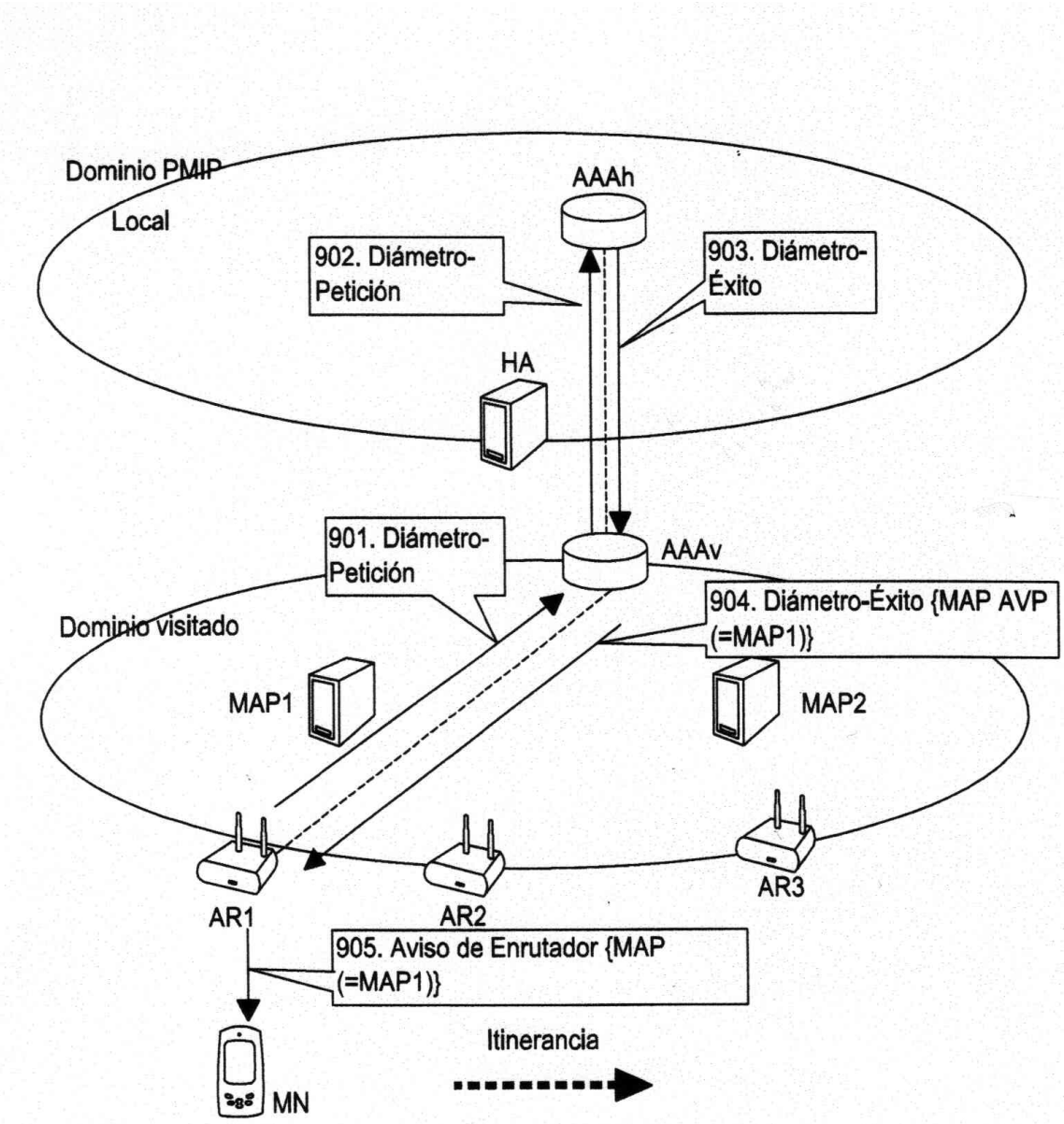
Dominio PMIP
Local
AAAh
902. Diámetro-Petición
903. Diámetro-Éxito
HA
901. Diámetro-Petición
AAAv
Dominio visitado
904. Diámetro-Éxito {MAP AVP (=MAP1)}
MAP1
MAP2
AR1
AR2
AR3
905. Aviso de Enrutador {MAP (=MAP1)}
Itinerancia
MN

Figura 9