(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 389 181**

(51) Int. CI.:

H04L 12/28 (2006.01)
H04L 29/08 (2006.01)
H04W 48/18 (2009.01)
H04W 48/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03741083 .4**
(96) Fecha de presentación: **30.06.2003**
(97) Número de publicación de la solicitud: **1639755**
(97) Fecha de publicación de la solicitud: **29.03.2006**

(54) Título: **Procedimiento de selección de red en redes de comunicaciones , red relacionada y productos de programa informático para el mismo**

(45) Fecha de publicación de la mención BOPI:
23.10.2012

(45) Fecha de la publicación del folleto de la patente:
23.10.2012

(73) Titular/es:
TELECOM ITALIA S.P.A. (100.0%)
PIAZZA DEGLI AFFARI, 2
20123 MILANO, IT

(72) Inventor/es:
ASCOLESE, ANTONIO;
COSTA, LUCIANA;
DELL'UOMO, LUCA;
RUFFINO, SIMONE y
SPINI, MARCO

(74) Agente/Representante:
PONTI SALES, Adelaida

DESCRIPCIÓN

Procedimiento de selección de red en redes de comunicaciones, red relacionada y producto de programa informático para el mismo.

Campo de la invención

[0001] La invención se refiere a procedimientos de selección de red para redes de comunicaciones, por ejemplo redes IP, tales como redes de área local (LAN) cableadas e inalámbricas. Más específicamente, la invención se refiere a disposiciones en las que una pluralidad de operadores de red comparten una red IP.

Descripción de la técnica relacionada

[0002] La posibilidad de que varios operadores de red y proveedores de servicios de Internet (ISP) estén presentes conjuntamente en una red IP, tal como una LAN inalámbrica (WLAN) y ofrezcan servicios de itinerancia (*roaming*) es un requisito clave para la implantación de una WLAN pública, como se describe por ejemplo en la especificación 3GPP TR 22.934 v 6.1.0 "*Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6)*" diciembre de 2002. Varios organismos reguladores nacionales también solicitan la capacidad de permitir itinerancia y permitir que un usuario elija una red apropiada.

[0003] Los procedimientos de acceso actualmente disponibles a redes de datos de proveedores de servicio solo tienen una flexibilidad muy limitada. De hecho, el proveedor de la red de acceso tiene normalmente contratos con otros proveedores de Internet. Los clientes de estos proveedores pueden acceder a las respectivas redes a través de las instalaciones de acceso a red del proveedor de la red de acceso. Normalmente, el operador que proporciona acceso a la red tiene a su vez acuerdos con otros proveedores u operadores; sin embargo, en muchos casos, el operador que proporciona acceso a la red a un determinado usuario no tiene un acuerdo de itinerancia directo con el operador local de ese usuario, sino solamente con uno o más terceros operadores que, a su vez, tienen acuerdos con el operador local del usuario.

[0004] Generalmente, los clientes de estos proveedores u operadores no tienen constancia de estos acuerdos. Cuando se encuentran en el área de cobertura de un proveedor de servicios inalámbricos de Internet (WISP) no tienen la posibilidad de saber a dónde se enviará la información de autenticación y, por lo tanto, qué redes de transporte transmitirán sus datos.

[0005] La Figura 1 representa un escenario de itinerancia correspondiente. Se muestran dos usuarios, A y B. Estos usuarios están abonados a servicios proporcionados por dos proveedores de servicio locales respectivos, concretamente HSPA y HSPB. Tanto A como B desean acceder a los servicios de sus HSP desde un proveedor de servicios de acceso genérico ASP a través de su red de acceso AN. El proveedor ASP puede tener un acuerdo de itinerancia directo con determinados proveedores de servicio visitados, tales como, por ejemplo, VSP1 y VSP2. Éstos, a su vez, pueden tener un acuerdo de itinerancia con HSPA. Sin embargo, estos últimos acuerdos pueden diferir, por ejemplo, en lo que respecta a los precios y la calidad de servicio (QoS) ofrecida. El proveedor de acceso ASP también puede tener un acuerdo de itinerancia directo con otro proveedor de servicios visitado VSP3, el cual tiene a su vez un acuerdo de itinerancia con HSPB. Por último, el proveedor de acceso ASP podría tener además un acuerdo directo con otro proveedor de servicios "local" de un usuario C, en concreto HSPC.

[0006] Durante la autenticación de clientes que solicitan acceso a la red de acceso AN, el proveedor de servicios de acceso ASP enviará una solicitud de autenticación a uno de los proveedores de servicio conectado directamente al mismo, en concreto VSP1, VSP2, VSP3 o HSPC. De hecho, el proveedor de servicios de acceso ASP no está en posición de autenticar los usuarios A y B localmente. En las disposiciones actuales, el proveedor de servicios de acceso ASP toma decisiones correspondientes de manera autónoma, sin recibir de los usuarios A o B ningún dato de entrada que no sea su identidad. Esta situación puede explicar los motivos por los que la publicidad de redes, es decir, anuncios de operadores de red disponibles en una WLAN pública dada, y la necesidad de seleccionar una red se describen en documentos tales como el 3GPP S2-031899 "*WLAN Network selection*", Conferencia de San Diego, del 12 al 16 de mayo de 2003 (www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_32_San_Diego/tdOCS) y el 3GPP TS 23.234 VI.10.0 : "*3rd Generation partmashup project; Technical Specification Group services and System Aspects; System description" (release 6)*", mayo de 2003.

[0007] Una disposición alternativa basada en el metalenguaje XML ha sido propuesta por el documento 3GPP S2-031864 "*Network Selection*", Conferencia de San Diego, del 12 al 16 de mayo de 2003 (www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_32_San_Diego/tdocs). La disposición correspondiente tiene la

desventaja de requerir una preconfiguración XML. Además, el código XML tiene una mayor cantidad de información de etiquetas, lo que requiere que se transmita una mayor cantidad de bits.

Objeto y resumen de la invención

[0008] Por lo tanto, el objeto de la presente invención es proporcionar una disposición que elimine los inconvenientes de las disposiciones de la técnica anterior mencionados anteriormente.

[0009] Según la presente invención, este objeto se consigue mediante un procedimiento que tiene las características descritas en la reivindicación independiente 1.

[0010] La presente invención también se refiere a una red de comunicaciones correspondiente definida en la reivindicación 12 y a un producto de programa informático que puede cargarse en la memoria de al menos un ordenador y que incluye partes de código software para llevar a cabo el procedimiento de la invención, como se define en la reivindicación 24. Evidentemente, la referencia a al menos un ordenador sirve para tener en cuenta que el procedimiento de la invención está adaptado para llevarse a cabo de manera descentralizada, donde diferentes tareas se asignan a diferentes ordenadores de una red.

[0011] En resumen, se describe una disposición en la que un usuario que desea acceder, a través de una red de acceso de terceros, a la red de uno de sus proveedores, puede elegir la(s) red(es) intermedia(s) a la(s) que se le(s) pasará la información de autenticación, entre otras cosas.

[0012] De esa manera, el usuario también podrá seleccionar la trayectoria que seguirán sus datos, en caso de que su proveedor tenga varios acuerdos de itinerancia con otros proveedores que, a su vez, tengan acuerdos con el proveedor que actúa como el proveedor de acceso.

[0013] Esta disposición es independiente de la tecnología de acceso implantada en la red de acceso. Ésta puede ser inalámbrica (por ejemplo, una red WLAN) o cableada (por ejemplo, una red PSTN con acceso por marcación). Por motivos de simplicidad, en lo que sigue se hará continuamente referencia a una LAN inalámbrica como un ejemplo preferido.

[0014] El proveedor que actúa como el proveedor de servicios de acceso es el encargado de comunicar las posibles alternativas a los usuarios, permitiéndoles de este modo tomar sus decisiones.

[0015] La disposición descrita en este documento soluciona, entre otras cosas, el problema de la publicidad de redes presente en el documento 3GPP SA2-031899 ya mencionado anteriormente.

[0016] Una realización preferida de la disposición descrita en este documento está basada en el denominado agente Diameter soportado en un protocolo base Diameter. La información básica relacionada se proporciona, por ejemplo, en el documento IETF draftietf-aaa-diameter-17.txt "*Diameter Base Protocol*", www.ietf.org. El agente Diameter se utiliza para proporcionar un marco de autenticación, autorización y contabilidad (AAA) para aplicaciones tales como acceso a red o movilidad IP. Esencialmente, un agente Diameter es un nodo Diameter que proporciona servicios de retransmisión, de delegación, de redireccionamiento o de conversión. Específicamente, la disposición descrita en este documento proporciona determinadas modificaciones realizadas en la manera en que el agente Diameter procesa solicitudes Diameter específicas y crea respuestas relativas cuando estas solicitudes de autenticación tienen un dominio desconocido.

[0017] Actualmente, estas solicitudes se descartan o, en el mejor de los casos, se reenvían a un servidor de autenticación por defecto. Con las modificaciones propuestas, un agente Diameter puede recuperar la información necesaria para procesar correctamente la solicitud de autenticación, dando de este modo al usuario la posibilidad de elegir el servidor de autenticación visitado al que el agente Diameter debe reenviar la solicitud.

[0018] Los expertos en la técnica apreciarán que la misma disposición también puede utilizarse con otros protocolos “AAA” tales como, por ejemplo, el protocolo denominado actualmente como servicio de usuario de acceso telefónico de autenticación remota (RADIUS); no soporta de manera explícita agentes, incluyendo los denominados apoderados (*proxies*), dispositivos de redireccionamiento y retransmisores. No se definirá el comportamiento esperado, ya que puede variar para diferentes implementaciones.

[0019] La lista de redes visitadas soportadas que tienen un acuerdo de itinerancia con determinados ISP “locales” del usuario se envía al usuario mediante el servidor de autenticación del proveedor que actúa como el proveedor de acceso. Esto sucede preferentemente durante el procedimiento de autenticación del usuario, utilizando un protocolo de autenticación extensible (EAP). Este protocolo de autenticación (descrito, por ejemplo, en el documento IETF draft-ietf-eap-rfc2284bis-03.txt, www.ietf.org), soporta múltiples mecanismos de autenticación y

normalmente se ejecuta directamente a través del enlace.

[0020] Con este objetivo, resulta conveniente una modificación del procedimiento EAP que consiste en añadir dos mensajes a la secuencia normal de paquetes intercambiados durante la autenticación. Sin embargo, el procedimiento propuesto debe soportarse por un mecanismo de autenticación genérico independientemente de la norma WLAN subyacente.

[0021] La principal ventaja de la disposición en cuestión radica en que no es necesario modificar el dispositivo de acceso local, ya que cualquier modificación puede implementarse en el terminal cliente y en los servidores AAA.

[0022] En una realización actualmente preferida de la invención, el usuario se identifica de manera unívoca mediante un identificador.

[0023] Éste puede ser, por ejemplo, el identificador de acceso a red, conocido como NAI, descrito, por ejemplo, en el documento RFC 2486 3GPP S2-031864 "*Network selection*", Conferencia de San Diego, del 12 al 16 de mayo de 2003 (www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS-2_32_San_Diego/tdOCS).

[0024] En una realización preferida de este tipo, el usuario envía sus credenciales a la red de acceso (lo que puede llevarse a cabo mediante un dispositivo cableado o un dispositivo inalámbrico). La red de acceso reenvía estas credenciales a un servidor de autenticación final, ubicado en el centro de datos del proveedor de servicios de acceso. El servidor de autenticación recupera las redes de itinerancia disponibles para ese usuario, identificado a través de la parte de dominio del NAI. Para realizar esta tarea, el servidor intercambia información con los servidores que pertenecen a los proveedores a los que está conectado. Como resultado, el servidor de autenticación recupera la lista de operadores que tienen un acuerdo de itinerancia con el (los) operador(es) del usuario. Este procedimiento se realiza solamente una vez cuando el servidor de autenticación recibe una primera solicitud de autenticación con respecto a un usuario para el que no existe ningún acuerdo de itinerancia directo con el proveedor de servicios local de tal usuario. El servidor de autenticación también reenvía, a través de la red de acceso, una lista de operadores al usuario. El usuario elige uno de los operadores de la lista recibida desde el servidor según sus preferencias o en función de algunos ajustes preconfigurados. Cuando se le presenta una lista de este tipo, el usuario enviará el identificador del operador elegido al servidor de autenticación de la red de acceso y el servidor de autenticación reenviará al proveedor elegido por el usuario la solicitud de autenticación, la cual contiene las credenciales del usuario.

[0025] Evidentemente, en caso de que el proveedor que actúa como el proveedor de acceso tenga un acuerdo de itinerancia directo con el proveedor de servicios local del usuario, el usuario recibirá una lista que comprende solamente un operador. Como alternativa, bajo estas circunstancias, el servidor de autenticación puede decidir simplemente reenviar directamente la solicitud de autenticación al proveedor de servicios local del usuario.

[0026] Después, el usuario llevará a cabo un procedimiento de autenticación habitual con su proveedor de servicios (por ejemplo, usando un mecanismo estándar como el EAP). Cuando se llevan a cabo las etapas de este procedimiento, la información de autenticación fluye a través de la red del operador elegido anteriormente. Específicamente, el servidor de autenticación reenviará mensajes de autenticación al servidor de autenticación visitado. Éste delegará a su vez tales mensajes al servidor del operador local, es decir, el servidor de autenticación local. Al tener la posibilidad de elegir el proveedor al cual el proveedor de servicios de acceso reenviará la solicitud de autenticación, los usuarios encaminarán sus flujos de datos con la consiguiente posibilidad de elegir, por ejemplo, en lo que respecta a los precios y la calidad de servicio (QoS) ofrecida.

Breve descripción de los dibujos

[0027] A continuación se describirá la invención, solamente a modo de ejemplo, haciendo referencia a las figuras adjuntas de los dibujos, en los que:

- la figura 1 se refiere tanto a la técnica anterior como a la invención, como ya se ha descrito anteriormente,
- la figura 2 es un diagrama que ilustra un modelo de interfuncionamiento simplificado,

- la figura 3 es un diagrama que ilustra un escenario de itinerancia específico,

- la figura 4 es un diagrama de bloques funcionales que representa de manera esquemática un procedimiento de selección de red generalizado,

- la figura 5 es un diagrama detallado de un procedimiento de selección de red en un interfuncionamiento WLAN,

- la figura 6 es un diagrama que ilustra una selección de red en acceso basado en web, y

- la figura 7 es otro diagrama de bloques funcionales que representa de manera esquemática un procedimiento de selección de red.

Descripción detallada de realizaciones preferidas de la invención

[0028] La descripción detallada a modo de ejemplo proporcionada en este documento se refiere a un procedimiento de selección de red aplicado a una red móvil pública terrestre (PLMN). Específicamente, se considerará como ejemplo un equipo de usuario que accede a un sistema 3GPP a través de una WLAN.

[0029] En términos generales, el procedimiento sigue los principios de selección de red descritos en el documento 3GPP TS 23.234 "*33GPP system to Wireless Local Area Network (WLAN) Interworking; System Description (Release 6)*".

[0030] La compartición de red de acceso de radio o la selección de proveedor se utiliza para la selección de red en un interfuncionamiento 3GPP-WLAN. En la figura 2 se presenta un modelo de interfuncionamiento simplificado en el que se muestran todos los participantes, es decir, un proveedor de servicios de Internet WLAN (WLAN ISP), un operador 3G visitado (VSP) y un operador 3G local (HSP).

[0031] Se supondrá que un abonado 3G desea utilizar los recursos y acceder a los servicios de su propia red de operador 3GPP respectiva.

[0032] El objetivo del interfuncionamiento 3G-WLAN es extender los servicios y la funcionalidad 3GPP al entorno de acceso WLAN. Por lo tanto, la WLAN se convierte efectivamente una tecnología de acceso de radio complementaria al sistema 3GPP. El interfuncionamiento 3G-WLAN es independiente de la tecnología de radio WLAN subyacente.

[0033] La WLAN proporciona acceso a servicios que pueden estar ubicados en la propia WLAN o en una red que esté conectada a la WLAN. Sin embargo, puede suponerse razonablemente que la WLAN no tiene acuerdos de itinerancia con todos los operadores 3G. Normalmente, el operador WLAN (o el proveedor de servicios WLAN) estará asociado tecnológicamente con un número limitado de operadores 3G (es decir, los operadores "visitados" VSP) para proporcionar conectividad hacia otras redes 3G (incluyendo el proveedor de red "local" desde el punto de vista del usuario).

[0034] Específicamente, se considerará un escenario del tipo ilustrado en la figura 3.

[0035] En la figura se muestra un área cubierta por un conjunto de proveedores de servicios de Internet WLAN (WISP) superpuestos designados como WISP1, WISP2 y WISP3, respectivamente. Cada uno de los proveedores WISP1, WISP2 y WISP3 se distingue posiblemente por diferentes canales WLAN y diferentes (y no exclusivos) acuerdos de itinerancia con varios operadores 3G 3G1, 3G2, 3G3.

[0036] Un usuario genérico que entra en esta área puede desear conectarse a su propia red "local" específica 3GA, 3GB o 3GC a la que está abonado/a. Hace esto para autenticarse y acceder a servicios ubicados en la propia WLAN o en una red conectada a la WLAN y que tiene un acuerdo específico con el operador 3G local.

[0037] La disposición descrita está destinada a dar al usuario la posibilidad de seleccionar una trayectoria de señalización para obtener autenticación y autorización de la red local. Cualquier flujo de datos de usuario posterior seguirá con gran probabilidad la misma trayectoria utilizada para la señalización. Por tanto, el usuario puede decidir entre diferentes acuerdos comerciales, por ejemplo en lo que respecta a los precios y a la calidad de servicio (QoS) ofrecida.

[0038] Haciendo referencia a la figura 3, el usuario que se abona a los servicios proporcionados al operador 3G 3GA puede llegar a la red local asociada de dos maneras diferentes, por ejemplo a través de cualquiera de los operadores visitados 3G1 y 3G2.

[0039] La técnica anterior no proporciona ningún mecanismo específico para decidir entre los dos.

[0040] Esto se aplica, por ejemplo, a la norma IEEE 802.11, pero observaciones similares se aplican a otras tecnologías WLAN. De hecho, en el caso de las WLAN según la norma IEEE 802.11, el nombre de red WLAN se transporta a través de la señal de baliza WLAN en el denominado elemento de información SSID (ID de conjunto de servicios). También existe la posibilidad de que un equipo de usuario (UE) solicite de manera activa soporte para los

SSID específicos enviando un mensaje de solicitud de sonda y recibiendo una respuesta si el punto de acceso soporta el SSID solicitado, como indica la norma IEEE 802.11. Sin embargo, en tales disposiciones de la técnica anterior, el usuario no tiene constancia del conjunto de redes visitadas soportadas y, por tanto, de la posibilidad de seleccionar la trayectoria para llegar al operador local deseado utilizando este mecanismo.

[0041] La disposición descrita en este documento sugiere un mecanismo para que el servidor de autenticación WISP envíe al usuario una lista de las redes visitadas soportadas que tienen un acuerdo de itinerancia con el proveedor local de servicios de Internet del usuario.

[0042] Esto sucede durante el procedimiento de autenticación del usuario, es decir, cuando un usuario envía sus credenciales.

[0043] En el caso del interfuncionamiento del sistema WLAN-3G, el soporte a ese respecto puede proporcionarse mediante un mecanismo de autenticación genérico (independientemente de la norma WLAN subyacente), tal como, por ejemplo, el protocolo de autenticación extensible denominado actualmente como EAP. En el caso de usuarios 3G, el mecanismo de autenticación que va a transportarse puede basarse por tanto, por ejemplo, en el mecanismo de autenticación EAP/AKA existente descrito en el borrador de Internet "draft-arkko-pppext-eap-aka-09.txt, "*EAP AKA Authentication*", febrero de 2003, www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-09. Como alternativa puede representarse mediante el mecanismo de autenticación EAP/SIM descrito en el borrador de Internet "draft-haverinen-pppext-eap-sim-10.txt", "*EAP SIM Authentication*", febrero de 2003, www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-10txt.

[0044] Se supondrá que el servidor de autenticación de acceso (AauS) correspondiente reside en el WISP (es decir, cualquiera de los elementos indicados como WISP1, WISP2 y WISP3 en la figura 3). Éste es normalmente un nodo Diameter con la función de un agente apoderado/de retransmisión Diameter (DRL).

[0045] Se supondrá que el servidor de autenticación visitado (VauS) reside en el operador 3G visitado (es decir, cualquiera de entre 3G1, 3G2 y 3G3 de la figura 3) y que es un nodo Diameter que actúa como un agente apoderado/de retransmisión Diameter (DRL) y también como un agente de redireccionamiento Diameter (DRD). Una implementación Diameter puede actuar como un tipo de agente para algunas solicitudes y como otro tipo de agente para otras. Un agente Diameter está presente por tanto en el VauS para actuar como:

- un agente apoderado/de retransmisión para aquellas solicitudes que deben reenviarse hacia un servidor de autenticación visitado (VauS) identificado en el AauS, y

- como un agente de redireccionamiento para aquellas solicitudes de autenticación que tienen un dominio desconocido.

[0046] El diagrama de la figura 5 detalla el procedimiento descrito a continuación.

[0047] Como una primera etapa, el dispositivo de red de acceso envía un mensaje de solicitud/identidad EAP al equipo de usuario (UE) para las credenciales del usuario. Los paquetes EAP se transportan a través de la interfaz LAN inalámbrica encapsulada dentro de cualquier protocolo específico de tecnología LAN inalámbrica.

[0048] Como una segunda etapa, el UE envía la identidad de usuario en un mensaje de respuesta/identidad EAP al dispositivo de red de acceso que se ajusta a un formato de identificador de acceso de red (NAI) especificado en la norma RFC2486. El NAI contiene el identificador que permite al AauS obtener el nombre de red local 3G. Por ejemplo, el UE puede enviar la identidad A de usuario como nombreusuario@HSPA.com o, para aquellos clientes que utilicen un módulo SIM como medio de identificación, como IMSI@HSPA.com.

[0049] Como una tercera etapa, el dispositivo de red de acceso reenvía el paquete de respuesta EAP del cliente a su AauS DRL de retransmisión. Normalmente, está encapsulado en un paquete Diameter con la identidad del cliente en el atributo Nombre de Usuario Diameter.

[0050] Tal y como se ha indicado, en la realización a modo de ejemplo considerada en este documento, el AauS es un agente apoderado/de retransmisión Diameter (DRL) adaptado para buscar el dominio en el mensaje de solicitud EAP Diameter. De hecho, no tendrá generalmente una entrada de encaminamiento en su tabla de encaminamiento Diameter para HSPA.com; esto se debe a que los acuerdos de itinerancia directos existen solamente con el VauS 1, el VauS 2, el VauS 3 y el proveedor de servicios local HSPC.

[0051] La tabla de encaminamiento, que normalmente está basada en dominios, está configurada de tal manera que todas las solicitudes de autenticación cuyo dominio no corresponde a ninguno de los presentes en la tabla de encaminamiento se redirigen a todos los VauS/DRD. Por tanto, el AauS envía una solicitud de redireccionamiento a todos los VauS/DRD y pone la solicitud del usuario en un estado pendiente. Esto es esencialmente la cuarta etapa del procedimiento considerado.

[0052] Como una quinta etapa subsiguiente, todos los VauS/DRD actúan en este caso como agentes de redireccionamiento que devuelven una notificación de redireccionamiento al AauS/DRL, con la información necesaria para llegar al servidor de autenticación local. La información relativa se inserta en una o más instancias del AVP (par de valores de atributo) Redireccionamiento-Ordenador Principal en el mensaje de respuesta.

[0053] Esencialmente, los siguientes eventos se producen en el escenario a modo de ejemplo que acaba de describirse.

[0054] El VauS1 (DRD) tiene un acuerdo de itinerancia con el proveedor de servicios local HSP A: por consiguiente, devuelve al AauS una notificación de redireccionamiento fijando el AVP Redireccionamiento-Ordenador_Principal = VauS 1. De esta manera, el AauS sabe que el VauS 1 puede reenviar la solicitud de autenticación al proveedor de servicios local HSPA. El valor VauS 1 del AVP se utiliza posteriormente por el AauS para formar la lista PLMN que se presenta al usuario para permitir la selección del operador preferido.

[0055] Además, el VauS 2 (DRD) tiene un acuerdo de itinerancia con el proveedor de servicios local HSP A: por consiguiente, devuelve al AauS una notificación de redireccionamiento fijando el AVP Redireccionamiento-Ordenador_Principal = VauS 2. De esta manera, el AauS sabe que el VauS 2 puede reenviar la solicitud de autenticación al proveedor de servicios local HSPA. El valor VauS 2 del AVP se utiliza posteriormente por el AauS para formar la lista PLMN que se presenta al usuario para permitir la selección del operador preferido.

[0056] El VauS 3 (DRD) no tiene ningún acuerdo de itinerancia con el proveedor de servicios local HSPA pero tiene un acuerdo de este tipo con el proveedor de servicios local HSPB, por lo que debe devolver una notificación de redireccionamiento con un AVP Redireccionamiento-Ordenador_Principal = Desconocido. De esta manera, el AauS sabe que el VauS 3 no podrá reenviar la solicitud de autenticación al proveedor de servicios local HSPA. El valor Desconocido del AVP se utiliza para indicar al AauS que no inserte el VauS 3 en la lista PLMN.

[0057] En la notificación de redireccionamiento puede incluirse otra información, tal como los AVP enumerados a continuación.

- AVP Utilización-Redireccionamiento-Ordenador_Principal: este AVP dictamina cómo el AauS/DRL va a utilizar la entrada de encaminamiento del AVP Redireccionamiento-Ordenador_Principal. Cuando está fijado a TODOS_LOS_DOMINIOS, todos los mensajes destinados al dominio solicitado se envían al ordenador principal especificado en el AVP Redireccionamiento-Ordenador_Principal. En el ejemplo descrito en este documento, todas las solicitudes de autenticación con dominio HSPA pueden enviarse por el AauS/DRL al VauS 1 o al VauS 2.

- AVP Redireccionamiento-Tiempo_Máximo_En_Caché: este AVP contiene el número máximo de segundos en que la entrada de tabla de encaminamiento, creada como resultado del AVP Redireccionamiento-Ordenador_Principal, estará almacenada en caché. Este AVP evita que el AauS tenga que interrogar todos los VauS/DRD si recibe de nuevo una solicitud de autenticación para algún dominio desconocido. Por ejemplo, en el ejemplo descrito en este documento, el AauS puede recibir al mismo tiempo más de una solicitud de autenticación con dominio "HSPA.com". De esta manera, ya tiene una lista VauS/PLMN disponible que enviar a los usuarios. Cuando el temporizador expira, el AauS repite, si fuera necesario, el proceso de redireccionamiento, actualizando de este modo las entradas de encaminamiento relacionadas con los acuerdos de itinerancia. El AauS puede enviar un mensaje de redireccionamiento no solicitado a todos los VauS/DRD de un dominio dado. El VauS puede contestar con un mensaje de respuesta de redireccionamiento no solicitado. Una alternativa es que el AauS espere una nueva solicitud de autenticación para el dominio particular y repetir el proceso de redireccionamiento solamente en este momento.

[0058] Cuando el AauS ha recibido notificaciones de redireccionamiento desde todos los VauS (DRD) está en condiciones de añadir una entrada de encaminamiento en la tabla basada en dominios para el dominio particular. En el ejemplo descrito en este documento, después del procedimiento de redireccionamiento, en la tabla de encaminamiento AauS habrá una entrada para el dominio HSPA en función de qué solicitudes de autenticación pueden reenviarse al VauS 1 o al Vaus 2.

[0059] Como se muestra en la figura 6, si el AauS recibe todas las notificaciones de redireccionamiento con el AVP Redireccionamiento-Ordenador_Principal = desconocido, entonces reenvía la solicitud de autenticación, recibida en la tercera etapa anterior, al Vaus especificado en la entrada por defecto de su tabla de encaminamiento.

Esta operación se llevará a cabo solamente tras la recepción de las notificaciones no satisfactorias.

[0060] Para la autenticación de otros usuarios HSPA, el AauS ya tiene una entrada, por lo que no es necesario ningún procedimiento de redireccionamiento; en este caso, el AauS busca la tabla de encaminamiento, encuentra la entrada ya presente y, después de completar la tercera etapa considerada anteriormente, procede directamente con la sexta etapa descrita anteriormente o con una variante de la misma.

[0061] La variante es cuestión se refiere al caso en que solamente un VauS puede reenviar la solicitud de autenticación al HSP pertinente, es decir, solo hay un VauS que tenga un acuerdo de itinerancia con tal HSP.

[0062] En el ejemplo descrito en este documento, cuando el usuario B envía su solicitud de autenticación (esto es esencialmente la tercera etapa considerada anteriormente), el AauS no tiene una entrada de encaminamiento para el dominio HSPB. Por lo tanto, utiliza un procedimiento de redireccionamiento para recuperar la información necesaria. En ese caso, el AauS recibe solamente un mensaje de redireccionamiento con un AVP Redireccionamiento-Ordenador_Principal válido. Este mensaje proviene del VauS 3, el único que tiene un acuerdo de itinerancia con el proveedor HSPB.

[0063] La posibilidad de elegir un operador preferido (PLMN) no existe para el usuario B; en consecuencia, el AauS puede reenviar directamente la credencial del usuario al VauS 3 tanto pronto como se reciba el mensaje de notificación de redireccionamiento. Para este fin, el AauS utiliza el campo “salto a salto” de la cabecera Diameter para encontrar la solicitud de autenticación del usuario en el estado pendiente que debe reenviarse.

[0064] Si, por el contrario, el usuario en cuestión tiene la posibilidad de elegir entre varios VauS/PLMN (es decir, existe más de un VauS que tiene un acuerdo de itinerancia con el HSP deseado), no es necesario que el AauS seleccione uno de los mismos como el destino del mensaje redirigido, sino que simplemente dará al usuario la posibilidad de elegirlo de la manera detallada a continuación. El AauS soportará una aplicación Diameter EAP con el fin de poder enviar la lista VauS (lista PLMN) al usuario a través de un paquete EAP encapsulado en un mensaje Diameter. El campo ‘salto a salto’ de la cabecera Diameter de la solicitud de autenticación en el estado pendiente se utiliza por el AauS para enviar un mensaje de solicitud Diameter/EAP, con un paquete EAP encapsulado en el mismo.

[0065] Este paquete EAP incluye la lista VauS/PLMN. El usuario elige el operador PLMN/VauS preferido y envía esta selección al AauS en un mensaje de respuesta Diameter-EAP. En función del dominio seleccionado por el usuario en el paquete EAP, el AauS reenvía el mensaje de solicitud/identidad Diameter EAP pendiente al VauS seleccionado por el usuario.

[0066] Debe definirse un tipo EAP específico para transportar la lista VauS/PLMN al usuario. En la figura 5, este tipo EAP se indica con xxx.

[0067] En el ejemplo descrito en este documento, el usuario A recibe la lista VauS/PLMN desde el AauS con la posibilidad de elegir VauS 1 o VauS 2 (estas operaciones comprenden esencialmente la sexta y la séptima etapas del procedimiento). El usuario A selecciona VauS 1 como la PLMN preferida y envía esta selección al AauS, comprendiendo esencialmente estas operaciones una octava y una novena etapas del procedimiento. Por último, el AauS reenvía la solicitud/identidad Diameter EAP al VauS1 que, a su vez, reenvía (lo que comprende esencialmente la décima etapa del procedimiento) la solicitud al proveedor HSPA para su autenticación.

[0068] Por lo tanto, se ha descrito una disposición en la que los identificadores de las redes disponibles en una WLAN se transmiten al usuario. El servidor de autenticación recupera las redes de itinerancia disponibles para ese usuario, identificado a través de, por ejemplo, la parte de dominio del identificador de acceso a red (NAI). Para llevar a cabo esta tarea, el servidor inicia un intercambio de información con todos los servidores que pertenecen a los proveedores a los que está conectado. Como resultado, el servidor de autenticación recupera la lista de los operadores que tienen un acuerdo de itinerancia con el operador local del usuario. Este procedimiento se lleva a cabo solamente una vez, es decir, en la primera solicitud de autenticación recibida por el servidor de autenticación para un usuario para el que no tiene un acuerdo de itinerancia directo con el proveedor local respectivo.

[0069] Después, el servidor de autenticación reenvía a través de la red de acceso la lista de operadores al usuario. El usuario elige uno de los operadores incluidos en la lista recibida desde el servidor, según sus preferencias locales o en función de algunos ajustes preconfigurados. En caso de que el proveedor de acceso tenga un acuerdo de itinerancia directo con el proveedor local en cuestión, el usuario recibirá una lista formada solamente por un operador, o el servidor de autenticación puede decidir reenviar directamente la solicitud de autenticación. El usuario devuelve al servidor de autenticación de la red de acceso el identificador del operador seleccionado. En este punto, el servidor de autenticación reenvía al proveedor elegido por el usuario la solicitud de autenticación, que contiene los credenciales del usuario.

[0070] Un posible uso alternativo de la invención es para una autenticación de usuario basada en web. Esto tiene la ventaja de extender el uso de esta solución a clientes que no soportan EAP.

[0071] El procedimiento se describe a continuación.

[0072] El usuario A solicita un servicio de un proveedor de servicios inalámbricos de Internet ISP, por ejemplo, "abriendo" un navegador web y solicitando posteriormente una URL. El dispositivo de red de acceso intercepta la solicitud del usuario y, a su vez, pide al usuario sus credenciales a través de una página HTML.

[0073] El usuario A envía su identidad (por ejemplo, en formato NAI) y la contraseña. Las credenciales se transportan al dispositivo de red de acceso utilizando HTTPS. El dispositivo de red de acceso las reenvía al servidor de autenticación de acceso (AauS) utilizando encapsulación Diameter. El servidor de autenticación de acceso (AauS) del WISP recupera las redes de itinerancia disponibles para ese usuario. Éstas se identifican a través de la parte de dominio del identificador NAI. Para realizar esta tarea, el servidor inicia un intercambio de información con todos los servidores que pertenecen a los proveedores a los que está conectado, como se ha descrito anteriormente.

[0074] Como resultado, el servidor de autenticación recupera la lista de operadores que tienen un acuerdo de itinerancia con el operador del usuario. El servidor de autenticación de acceso (AauS) envía esta lista de operadores al usuario.

[0075] En caso de que el proveedor de servicios de acceso ASP tenga un acuerdo de itinerancia directo con el proveedor de servicios local deseado HSP, el usuario recibirá una lista que incluye solamente un operador; como alternativa, el servidor de autenticación puede decidir reenviar directamente la solicitud de autenticación.

[0076] La lista se presenta al usuario con una nueva página HTML con enlaces de selección de redes IP. El usuario elige uno de los operadores incluidos en la lista recibida desde el servidor.

[0077] En este punto, el servidor de autenticación reenvía la solicitud de autenticación, que contiene las credenciales del usuario, al proveedor elegido por el usuario. El servidor de autenticación local acepta las credenciales el usuario, comprueba la identidad del usuario para su validación y si la autenticación es satisfactoria, ordena al servidor de autenticación de acceso que proporcione el servicio de usuario. El procedimiento correspondiente se ilustra en la figura 7.

[0078] La disposición descrita se basa en el uso de agentes Diameter. Evidentemente, pueden utilizarse de manera satisfactoria otros protocolos "AAA", tales como Radius, incluso aunque algunos de estos no puedan proporcionar un soporte explícito para agentes, incluyendo apoderados, dispositivos de redireccionamiento y retransmisores.

[0079] Por consiguiente, sin perjuicio del principio subyacente de la invención, los detalles y las realizaciones pueden variar, también de manera significativa, con respecto a lo que se ha descrito anteriormente, simplemente a modo de ejemplo, sin apartarse del alcance de la invención definida por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento para proporcionar a al menos un usuario (A, B, C) acceso a un operador local respectivo (HSPA, HSPB, HSPC) a través de una red de comunicaciones, estableciéndose dicho acceso a través de una red de acceso (AN, ASP) y a través de cualquiera de una pluralidad de redes visitadas soportadas (VSP1, VSP2, VSP3), donde al menos una de dichas redes visitadas soportadas (VSP1, VSP2, VSP3) comprende un agente apoderado/de retransmisión para aquellas solicitudes de autenticación que deben reenviarse a un operador identificado y un agente de redireccionamiento para aquellas solicitudes de autenticación que tienen un dominio desconocido, por lo que dicho usuario (A, B, C) tiene la posibilidad de seleccionar una de dichas redes visitadas soportadas (VSP1, VSP2, VSP3) como la trayectoria para llegar a dicho operador local respectivo (HSPA, HSPB, HSPC), incluyendo el procedimiento las etapas de:

- recibir de dicho usuario (A, B, C) credenciales de usuario en dicha red de acceso (AN, ASP),

- reenviar dichos credenciales de usuario a una función de autenticación en dicha red de acceso (AN, ASP),

- recuperar un conjunto de redes de itinerancia disponibles (VSP1, VSP2, VSP3) para dicho usuario (A, B, C) recuperando de este modo una lista de operadores que tienen un acuerdo de itinerancia con dicho operador local respectivo (HSPA, HSPB, HSPC) de dicho usuario (A, B, C),

- reenviar dicha lista a dicho usuario (A, B, C);

- recibir de dicho usuario (A, B, C) en dicha función de autenticación un identificador de un operador seleccionado de dicha lista, y

- reenviar al operador identificado mediante dicho identificador una solicitud de autenticación del usuario; **caracterizado porque** incluye además las etapas de:

- redirigir a todas dichas redes visitadas soportadas (VauS/DRD) las solicitudes de autenticación cuyo dominio no corresponde a ningún dominio identificado en dicha red de acceso (AauS/DRL), y

- devolver desde dichas redes visitadas soportadas (VauS/DRD) a dicha red de acceso (AauS/DRL) notificaciones de redireccionamiento así como información de contacto a dicho operador local respectivo del usuario.

2. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de incluir las credenciales de usuario en dicha solicitud de autenticación del usuario.

3. El procedimiento de la reivindicación 1, **caracterizado porque** incluye las etapas de:

- asignar a dicho usuario (A, B, C) un identificador NAI,

- identificar dicho usuario (A, B, C) a través de la parte de dominio de dicho identificador NAI.

4. El procedimiento de la reivindicación 1, **caracterizado porque** dichas etapas de recibir y reenviar credenciales de usuario y de recuperar un conjunto de redes de itinerancia disponibles se llevan a cabo una sola vez, cuando dicha función de autenticación recibe una primera solicitud de autenticación con respecto a un usuario para el que no existe ningún acuerdo de itinerancia directo con dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario.

5. El procedimiento de la reivindicación 1, **caracterizado porque**, cuando dicha red de acceso (AN, ASP) tiene un acuerdo de itinerancia directo con dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario, incluye la etapa de reenviar a dicho usuario (A, B, C) una lista que incluye solamente dicho operador local respectivo del usuario.

6. El procedimiento de la reivindicación 1, **caracterizado porque**, cuando dicha red de acceso (AN, ASP) tiene un acuerdo de itinerancia directo con dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario, incluye la etapa de reenviar directamente la solicitud de autenticación del usuario a dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario.

7. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de delegar dicha solicitud de autenticación del usuario desde dicho operador identificado mediante dicho identificador a dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario.

8. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de seleccionar dicha función de autenticación como una función basada en EAP.

9. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de incluir en al menos una de dicha red de acceso (WISP1, WISP32, WISP3) y dichas redes visitadas soportadas (VSP1, VSP2, VSP3) un nodo Diameter.

10. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de incluir en al menos una de dicha red de acceso (WISP1, WISP2, WISP3) y dichas redes visitadas soportadas (VSP1, VSP2, VSP3) un agente apoderado/de retransmisión (DRL).

11. El procedimiento de la reivindicación 1, **caracterizado porque** incluye la etapa de incluir en al menos una de dichas redes visitadas soportadas (VSP1, VSP2, VSP3) un agente de redireccionamiento (DRD).

12. Una red de comunicaciones dispuesta para proporcionar a al menos un usuario (A, B, C) acceso a un operador local respectivo (HSPA, HSPB, HSPC) a través de una red de acceso (AN, ASP) y a través de cualquiera de una pluralidad de redes visitadas soportadas (VSP1, VSP2, VSP3), donde al menos una de dichas redes visitadas soportadas (VSP1, VSP2, VSP3) incluye un agente apoderado/de retransmisión para aquellas solicitudes de autenticación que deben reenviarse a un operador identificado y un agente de redireccionamiento para aquellas solicitudes de autenticación que tienen un dominio desconocido, por lo que dicho usuario (A, B, C) tiene la posibilidad de seleccionar una de dichas redes visitadas soportadas (VSP1, VSP2, VSP3) como la trayectoria para llegar a dicho operador local respectivo (HSPA, HSPB, HSPC), donde:

dicha red de acceso (AN, ASP) está configurada para recibir de dicho usuario (A, B, C) credenciales de usuario y para reenviar dichas credenciales de usuario a dicho servidor de autenticación,

- dicho servidor de autenticación está configurado para recuperar un conjunto de redes de itinerancia disponibles (VSP1, VSP2, VSP3) para dicho usuario (A, B, C) recuperando de este modo una lista de operadores que tienen un acuerdo de itinerancia con dicho operador local respectivo (HSPA, HSPB, HSPC) de dicho usuario (A, B, C) y para reenviar dicha lista a dicho usuario (A, B, C),

- dicho servidor de autenticación está configurado para recibir de dicho usuario (A, B, C) un identificador de un operador seleccionado de dicha lista y para reenviar al operador identificado mediante dicho identificador una solicitud de autenticación del usuario;

caracterizada porque dicha red de acceso (WISP1, WISP2, WISP3) está configurada para redirigir a todas dichas redes visitadas soportadas (VauS/DRD) las solicitudes de autenticación cuyo dominio no corresponde a ningún dominio identificado en dicha red de acceso (AauS/DRL) y **porque** dichas redes visitadas soportadas (VauS/DRD) están configuradas para devolver a dicha red de acceso (AauS/DRL) notificaciones de redireccionamiento así como información de contacto a dicho operador local respectivo del usuario.

13. La red de comunicaciones de la reivindicación 12, **caracterizada porque** dicho servidor de autenticación está configurado para incluir las credenciales de usuario en dicha solicitud de autenticación del usuario.

14. La red de comunicaciones de la reivindicación 12, **caracterizada porque** dicho usuario (A, B, C) se identifica mediante un identificador NAI y dicha red de acceso (AN, ASP) está configurada para identificar dicho usuario (A, B, C) a través de la parte de dominio de dicho identificador NAI.

15. La red de comunicaciones de la reivindicación 12, **caracterizada porque** dicho servidor de autenticación está configurado para recibir y reenviar credenciales de usuario y para recuperar un conjunto de redes de itinerancia disponibles solamente una vez, cuando dicho servidor de autenticación recibe una primera solicitud de autenticación con respecto a un usuario para el que no existe ningún acuerdo de itinerancia directo con dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario.

16. La red de comunicaciones de la reivindicación 12, **caracterizada porque** dicha red de acceso (AN, ASP) tiene un acuerdo de itinerancia directo con dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario, y dicha red de acceso (AN, ASP) está configurada para reenviar a dicho usuario (A, B, C) una lista que incluye solamente dicho operador local respectivo del usuario.

17. La red de comunicaciones de la reivindicación 12, **caracterizada porque** dicha red de acceso (AN, ASP) tiene un acuerdo de itinerancia directo con dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario, y dicha red de acceso (AN, ASP) está configurada para reenviar directamente la solicitud de autenticación del

usuario a dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario.

18. La red de comunicaciones de la reivindicación 12, **caracterizada porque** dichas redes visitadas soportadas (VSP1, VSP2, VSP3) están configuradas para delegar dicha solicitud de autenticación del usuario desde dicho operador identificado mediante dicho identificador a dicho operador local (HSPA, HSPB, HSPC) respectivo del usuario.

19. La red de comunicaciones de la reivindicación 12, **caracterizada porque** dicho servidor de autenticación es un servidor basado en EAP.

20. La red de comunicaciones de la reivindicación 12, **caracterizada porque** al menos una de dicha red de acceso (WISP1, WISP2, WISP3) y dichas redes visitadas soportadas (VSP1, VSP2, VSP3) está configurada como un nodo Diameter.

21. La red de comunicaciones de la reivindicación 12, **caracterizada porque** al menos una de dicha red de acceso (WISP1, WISP2, WISP3) y dichas redes visitadas soportadas (VSP1, VSP2, VSP3) incluye un agente apoderado/de retransmisión (DRL).

22. La red de comunicaciones de la reivindicación 12, **caracterizada porque** al menos una de dichas redes visitadas soportadas (VSP1, VSP2, VSP3) incluye un agente de redireccionamiento (DRD).

23. La red de comunicaciones de la reivindicación 12, bajo la forma de una red IP.

24. Un producto de programa informático que puede cargarse en la memoria de al menos un ordenador y que incluye partes de código software para llevar a cabo las etapas de cualquiera de las reivindicaciones 1 a 11.

Fig. 1

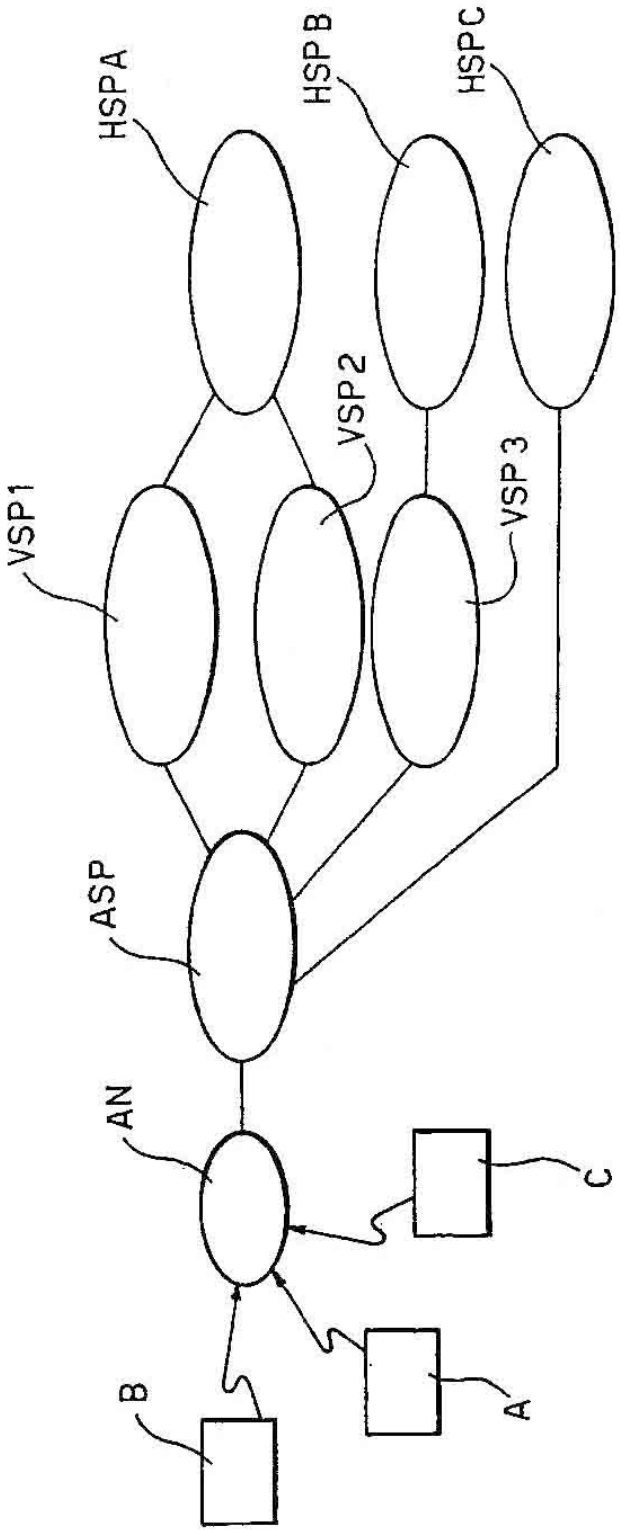
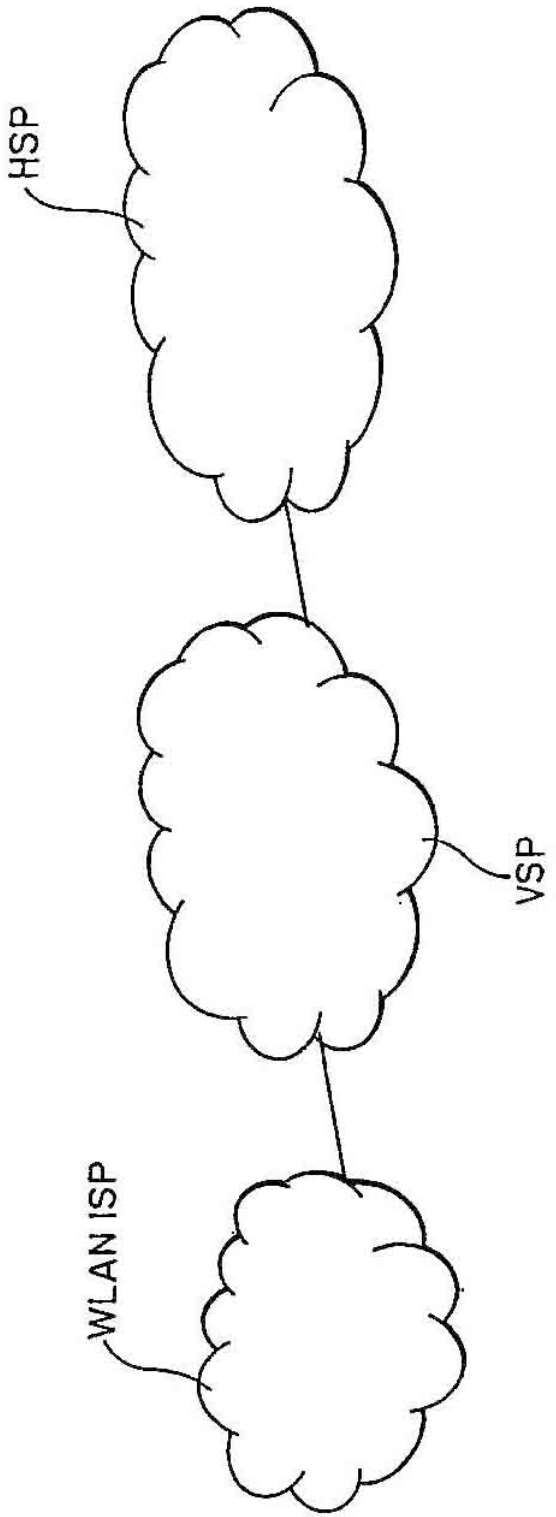


Fig. 2



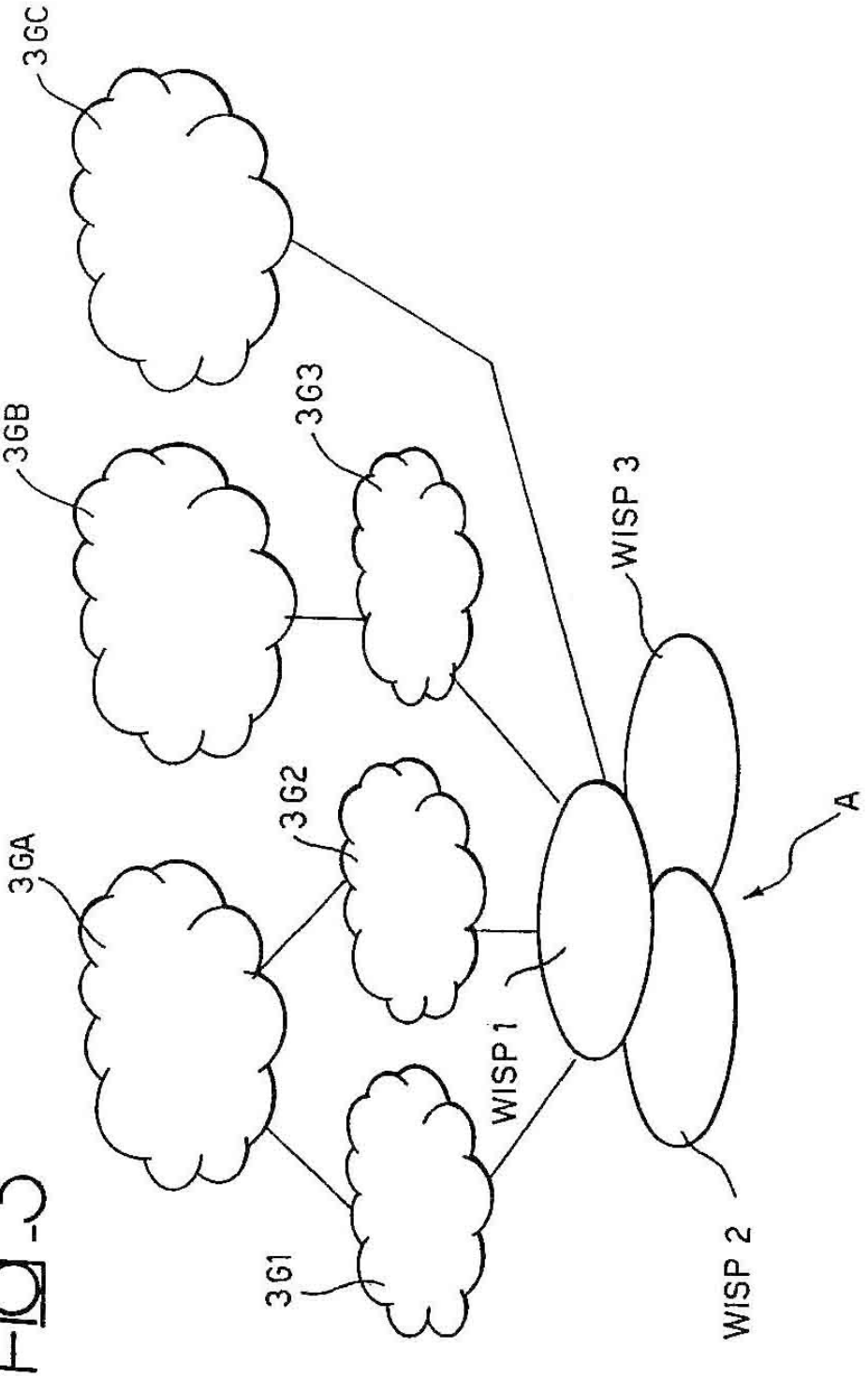


Fig. 3

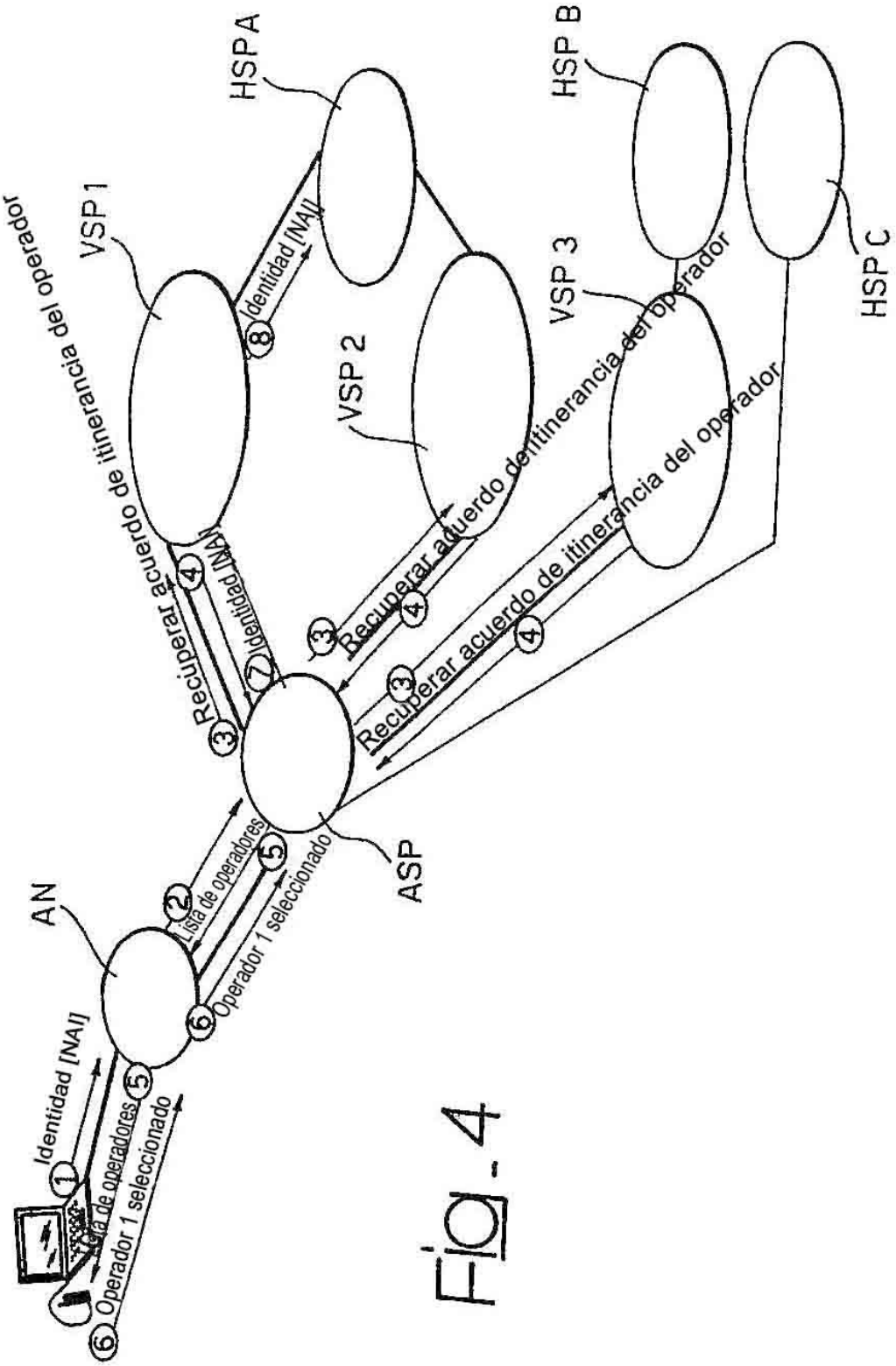

HSP A
HSP B
VSP 1
VSP 2
VSP 3
HSP C
AN
ASP
Identidad [NAI]
Lista de operadores
Operador 1 seleccionado
Recuperar acuerdo de itinerancia del operador
Recuperar acuerdo de itinerancia del operador
Recuperar acuerdo de itinerancia del operador
Identidad [NAI]
Identidad [NAI]
Lista de operadores
Operador 1 seleccionado

Fig. 4

FIG-5

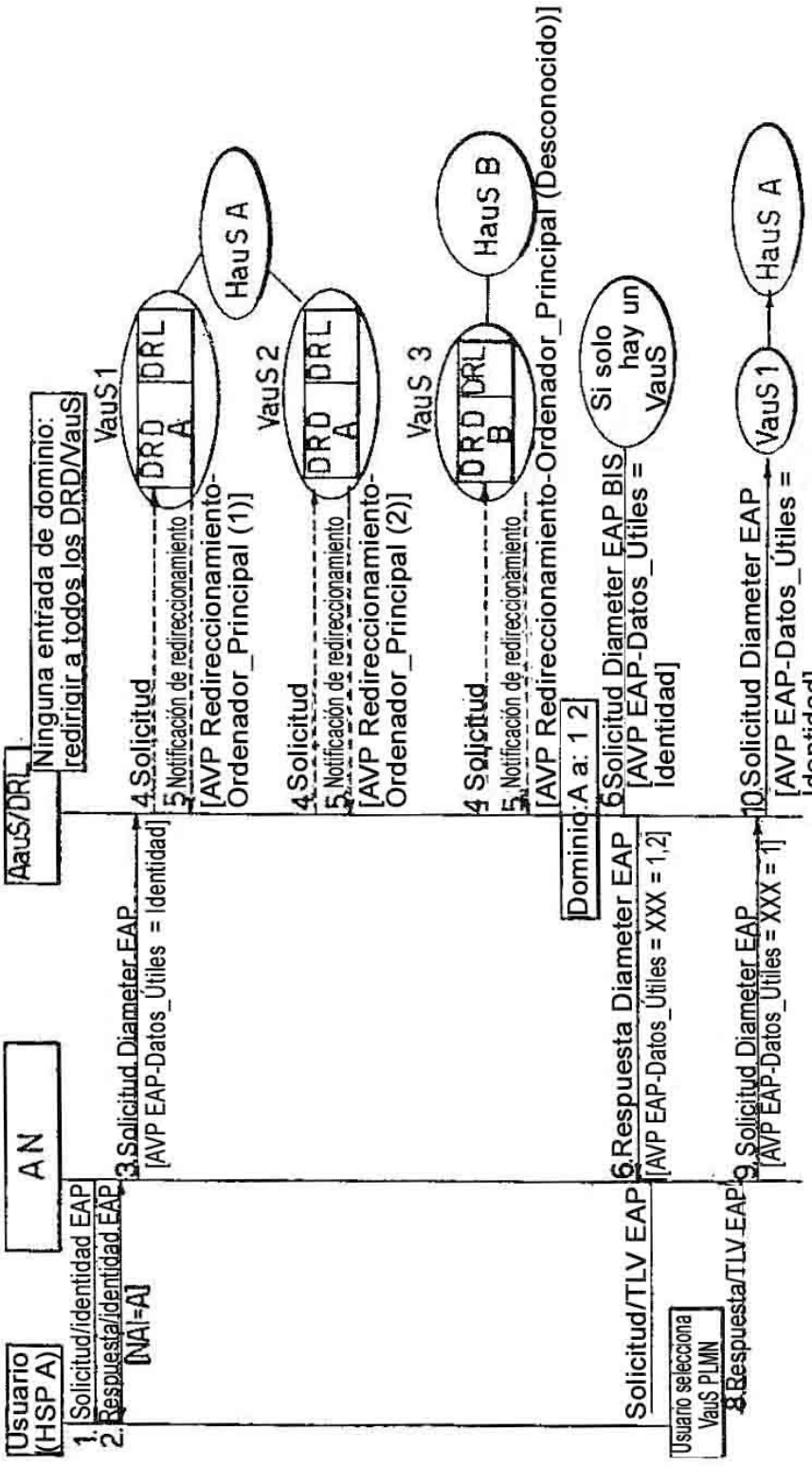

Usuario (HSP A)
AN
AauS/DRL
VauS 1
VauS 2
VauS 3
HauS A
HauS B
1. Solicitud/identidad EAP
2. Respuesta/identidad EAP [NAI=A]
3.Solicitud Diameter EAP [AVP EAP-Datos_Útiles = Identidad]
Ninguna entrada de dominio: redirigir a todos los DRD/VauS
4.Solicitud
5.Notificación de redireccionamiento [AVP Redireccionamiento-Ordenador_Principal (1)]
DRD A
DRL
4.Solicitud
5.Notificación de redireccionamiento [AVP Redireccionamiento-Ordenador_Principal (2)]
DRD A
DRL
4 Solicitud
5. Notificación de redireccionamiento [AVP Redireccionamiento-Ordenador_Principal (Desconocido)]
DRD B
DRL
Dominio A a: 1 2
6.Solicitud Diameter EAP BIS [AVP EAP-Datos_Útiles = Identidad]
Si solo hay un VauS
6.Respuesta Diameter EAP [AVP EAP-Datos_Útiles = XXX = 1,2]
Solicitud/TLV EAP
Usuario selecciona VauS PLMN
8.Respuesta/TLV EAP
9.Solicitud Diameter EAP [AVP EAP-Datos_Útiles = XXX = 1]
10.Solicitud Diameter EAP [AVP EAP-Datos_Útiles = Identidad]
VauS 1
HauS A

Fig.6

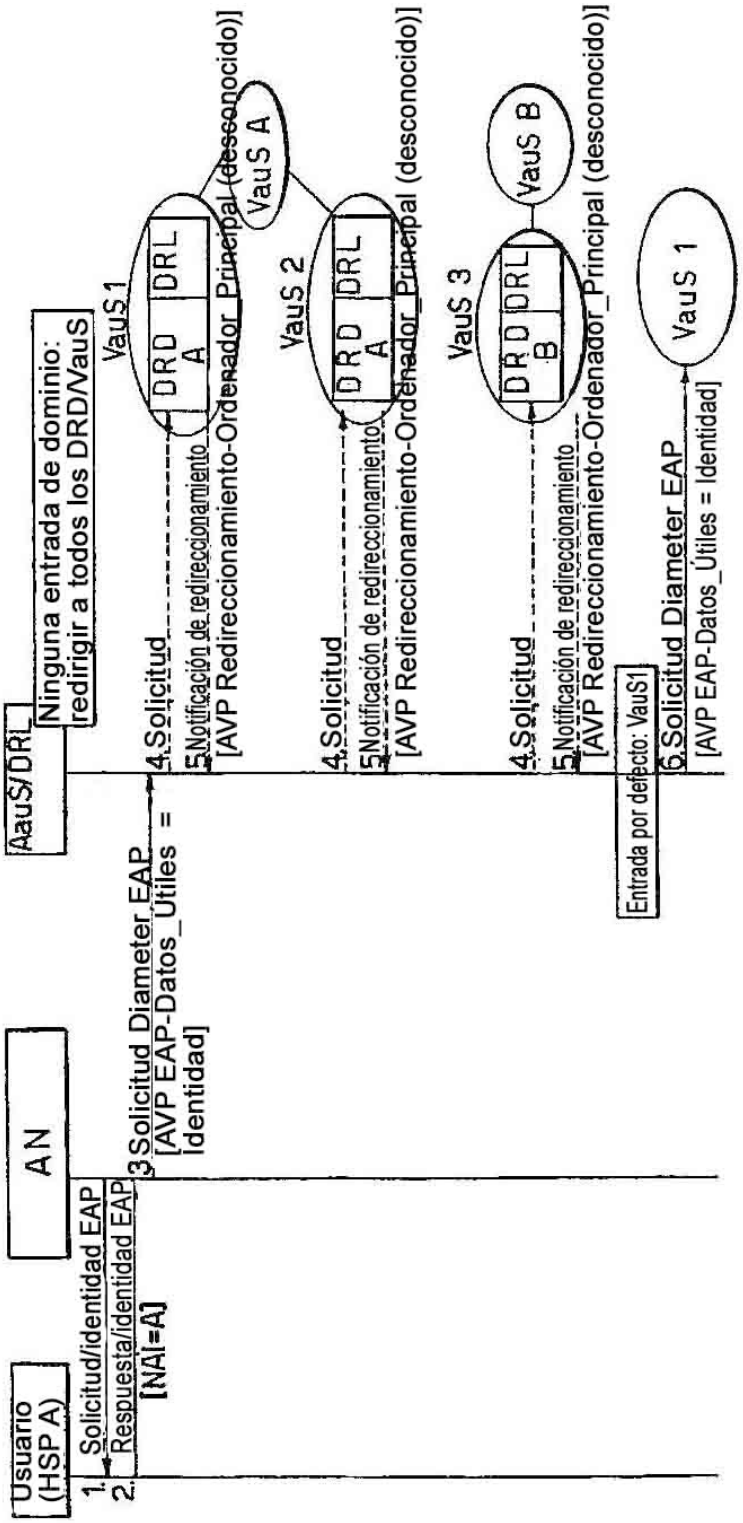
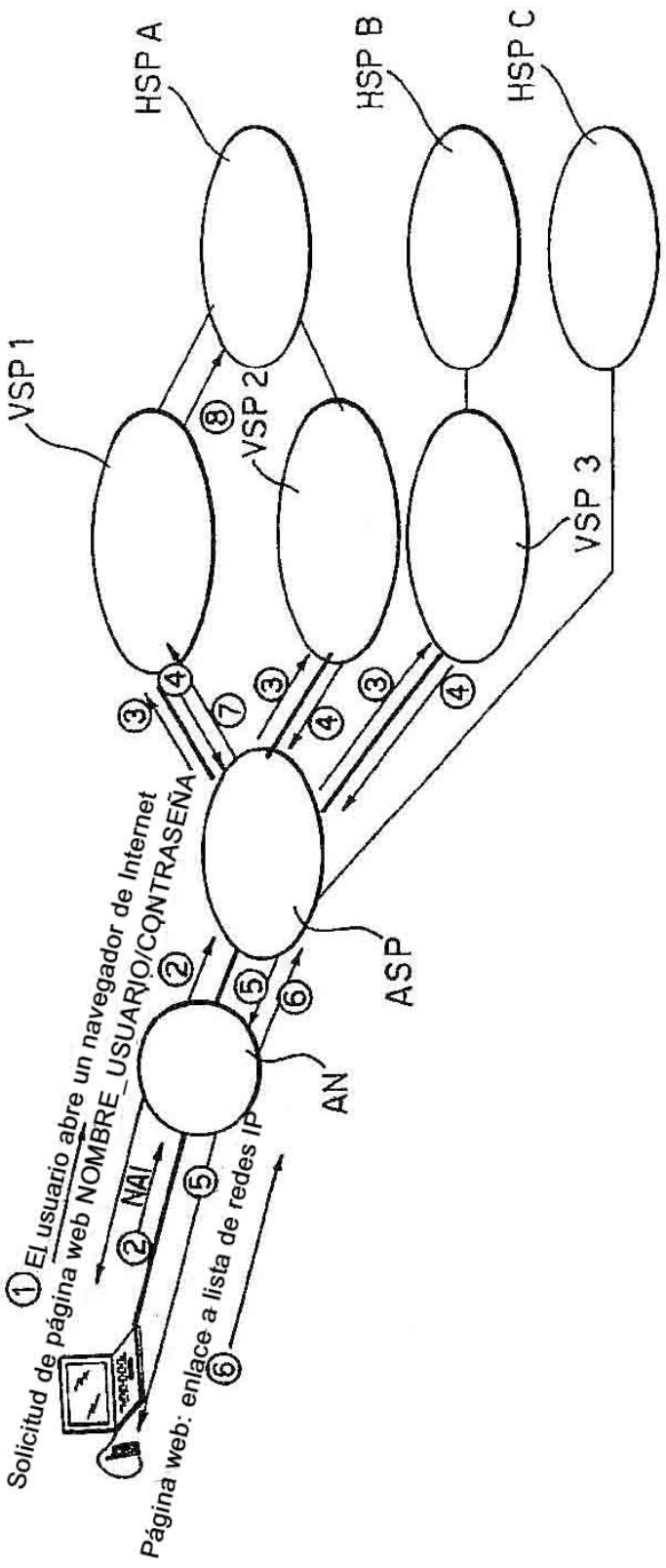

Usuario (HSP A)
AN
AauS/DRL
1. Solicitud/identidad EAP
2. Respuesta/identidad EAP
[NAI=A]
3 Solicitud Diameter EAP
[AVP EAP-Datos_Útiles = Identidad]
Ninguna entrada de dominio: redirigir a todos los DRD/VauS
VauS 1
DRD A
DRL
4.Solicitud
5.Notificación de redireccionamiento
[AVP Redireccionamiento-Ordenador_Principal (desconocido)]
VauS A
VauS 2
DRD A
DRL
4.Solicitud
5.Notificación de redireccionamiento
[AVP Redireccionamiento-Ordenador_Principal (desconocido)]
VauS 3
DRD B
DRL
4.Solicitud
5.Notificación de redireccionamiento
[AVP Redireccionamiento-Ordenador_Principal (desconocido)]
VauS B
Entrada por defecto: VauS1
6.Solicitud Diameter EAP
[AVP EAP-Datos_Útiles = Identidad]
VauS 1

Fig. 7


HSP A
HSP B
HSP C
VSP 1
VSP 2
VSP 3
ASP
AN
NAI
1 El usuario abre un navegador de Internet
Solicitud de página web NOMBRE_USUARIO/CONTRASEÑA
2
3
4
5
6
7
8
Página web: enlace a lista de redes IP