(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 539 271**

(51) Int. CI.:

H04M 3/44 (2006.01)
H04M 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.07.2005 E 05254364 (2)**

(97) Fecha y número de publicación de la concesión europea: **18.03.2015 EP 1617641**

(54) Título: **Sistema y método para marcar rápidamente en una red privada virtual**

(30) Prioridad:

13.07.2004 GB 0415650

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.06.2015

(73) Titular/es:

VODAFONE GROUP PLC (100.0%)
VODAFONE HOUSE THE CONNECTION
NEWBURY, BERKSHIRE RG14 2FN, GB

(72) Inventor/es:

MURRAY, RICHARD y
HUDSON, NICK

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y método para marcar rápidamente en una red privada virtual

La presente invención se refiere a un sistema de comunicaciones que incluye una pluralidad de redes de telecomunicaciones. Las redes proporcionan terminales de abonado con números de teléfono conocidos públicamente. Cada red permite que terminales de abonado seleccionados registrados con la misma sean asociados juntos en un grupo (por ejemplo un plan de marcación privado o red privada virtual (VPN)). Esto puede permitir a esos terminales de abonado dirigir las comunicaciones entre sí usando un código respectivo asignado a cada uno de los terminales de abonado seleccionados. Por ejemplo, este puede ser un código de marcación corta o un código que corresponde a un número de extensión usado también para hacer llamadas de teléfono internas en una red telefónica fija.

Se conoce para una red de telecomunicaciones móviles dotar a abonados seleccionados (por ejemplo, aquellos que pertenecen a una organización o compañía particular) con un plan de marcación privado o VPN. Los abonados dentro de la VPN pueden dirigir las comunicaciones entre sí usando un código que es diferente al número de teléfono conocido públicamente asignado a cada uno de los terminales de abonado. El código típicamente será un código de marcación corta (por ejemplo, un código de cuatro dígitos que corresponde al número de extensión del usuario del terminal de abonado en la red de comunicaciones interna fija de la organización). Además o alternativamente, los terminales de abonado dentro de la VPN se pueden dotar con servicios especiales no disponibles fuera de la VPN y se pueden tarificar por la red de telecomunicaciones móviles de una forma diferente de los abonados que no están en la VPN.

Mientras que tales disposiciones son convenientes, tales sistemas solamente permiten a los abonados de la red que aloja la VPN acceder a la VPN (es decir, ser capaz de dirigir llamadas a otros terminales de abonado usando los códigos).

La EP1113661A2 describe una red telefónica de protocolo de Internet y red pública telefónica conmutada, en la que se pueden definir grupos cerrados de usuarios. Los miembros de los grupos cerrados de usuarios pueden dirigir comunicaciones entre sí usando códigos de marcación corta y pueden estar sujetos a disposiciones de facturación especiales. La afiliación de los grupos se puede definir y ajustar dinámicamente por los miembros del grupo, el proveedor de servicios de telefonía o una fuente externa tal como una organización externa a la red. Un grupo cerrado de usuarios puede comprender uno o más miembros conectados a la red de telefonía de protocolo de Internet y uno o más miembros conectados a la red pública telefónica conmutada. Una base de datos contiene el código de marcación corta de cada uno de los miembros y el DN y/o dirección IP correspondiente de cada código de marcación corta. En uso, un miembro que llama de un grupo cerrado de usuarios marca un código de marcación corta de un miembro llamado del grupo. Un gestor de llamadas entonces recibe los dígitos marcados y determina la identidad de la parte llamada accediendo a la base de datos.

La US2001/0005414A1 describe un método de encaminamiento de tráfico desde una parte que llama en una primera VPN inalámbrica definida geográficamente sobre un primer acceso local y área de transporte (LATA) a una parte llamada en una segunda VPN inalámbrica definida geográficamente sobre una segunda LATA. Las primera y segunda VPN tienen respectivamente un primer y segundo punto de conmutación de servicio (SSP) y un primer y segundo concentrador. Un punto de control de conmutación (SCP) puede comunicar con los SSP y los concentradores. Una línea de vínculo conecta los concentradores. Cuando una parte que llama marca el código de marcación corta de una parte llamada, el primer SSP recibe el código de marcación y envía una consulta al SCP. El SCP determina que la llamada es para una parte llamada en una segunda VPN y convierte el código de marcación corta a un número de encaminamiento traducido. Entonces responde a la consulta proporcionando el miembro de encaminamiento traducido y también un número de encaminamiento del primer concentrador, al primer SSP. El primer SSP entonces encamina la llamada al primer concentrador y, además, envía un mensaje de dirección inicial al primer concentrador que incluye el número de encaminamiento traducido y el número de encaminamiento del primer concentrador. El primer concentrador entonces obtiene a partir del SCP el código de marcación corta, la información de facturación y la identidad del grupo troncal primario que especifica la línea de vínculo. El concentrador entonces encamina la llamada sobre la línea de vínculo al segundo concentrador, incluyendo el envío del código de marcación corta. El segundo concentrador entonces envía el código de marcación corta al SCP y obtiene el código de encaminamiento traducido. El segundo concentrador encamina posteriormente la llamada al segundo SSP, que encamina la llamada hacia delante a la parte llamada.

Según un primer aspecto de la presente invención, se proporciona un sistema de comunicaciones que incluye una pluralidad de redes de telecomunicaciones inalámbricas, cada una que incluye una red de acceso radio y una red central, como se define en la reivindicación 1.

Proporcionando la base de datos de códigos y números de teléfono conocidos públicamente correspondientes de cada una de las redes, esto permite que un terminal de abonado de un grupo (por ejemplo, una VPN) dentro de una red sea capaz de dirigir un terminal a otro grupo (por ejemplo, otra VPN) en otra red usando el código de ese otro terminal.

Según un segundo aspecto de la presente invención, se proporciona un método de habilitación de comunicación entre una pluralidad de redes de telecomunicaciones inalámbricas, cada red que incluye una red de acceso radio y una red central, como se define en la reivindicación 17.

Aspectos adicionales de la invención se definen en las reivindicaciones dependientes.

Para una mejor comprensión de la presente invención se describirá ahora una realización a modo de ejemplo, con referencia a los dibujos anexos, en los que:

La Figura 1 es un dibujo esquemático de dos redes de telefónicas móviles para uso en la explicación de la operación de esas redes, las disposiciones de "tránsito" entre las dos redes y cómo se manejan los códigos para una VPN;

La Figura 2 muestra el intercambio de datos entre los elementos mostrados en la Figura 1 cuando un abonado a una VPN administrada por una red doméstica llama a otro abonado en esa VPN;

La Figura 3 muestra el intercambio de datos entre los elementos mostrados en la Figura 1 cuando un abonado a una VPN administrada por una red doméstica llama a un abonado en esa VPN que está "transitando";

La Figura 4 muestra el intercambio de datos que ocurre entre los elementos mostrados en la Figura 1 cuando un abonado a la VPN administrada por una red doméstica desea hacer una llamada a otro abonado de la VPN cuando el abonado que llama está "transitando";

La Figura 5 muestra datos de ejemplo para dos VPN alojadas por la red A de la Figura 1;

La Figura 6 es un dibujo esquemático de dos redes telefónicas móviles similares a las de la Figura 1 pero mostrando los elementos adicionales proporcionados según la invención;

La Figura 7 muestra en más detalle las conexiones entre una base de datos VPN central y los elementos de las redes A y B mostradas en la Figura 6 y los intercambios de datos que ocurren entre los mismos;

La Figura 8 muestra la arquitectura de la base de datos de VPN central;

La Figura 9 muestra ejemplos de datos de VPN almacenados por la base de datos de VPN central;

La Figura 10 muestra ejemplos de datos "arrastrados" por la red A desde la base de datos de VPN central almacenada por esa red junto con datos para las VPN alojadas por la red A;

La Figura 11 ilustra una disposición alternativa, pero similar, a la Figura 10, donde las VPN se identifican separadamente; y

La Figura 12 muestra el intercambio de datos entre los elementos mostrados en la Figura 6 cuando un abonado de una VPN administrada por una red llama a un abonado de una VPN administrada por otra red.

En los dibujos elementos iguales se designan de manera general con los mismos números de referencia.

La Figura 1 explica esquemáticamente la operación de dos redes GSM entre las cuales hay un acuerdo de tránsito. La red A tiene la facilidad de proporcionar una red privada virtual (VPN) para grupos de sus abonados. Un grupo de abonados en una VPN se puede dotar con facilidades adicionales. Por ejemplo, se puede dar un número de código a cada abonado en una VPN además del número de teléfono móvil convencional (el MSISDN – número de ISDN Internacional de Estación Móvil). Este número de código típicamente será de una longitud fija y significativamente más corto que un MSISDN. Por ejemplo, el número puede ser un número de cuatro dígitos en forma de un número de extensión asignado en la centralita telefónica de la organización para la cual se proporciona la VPN.

Es conocido proporcionar este tipo de VPN a abonados de un sistema de telecomunicaciones móviles. Dotando a los terminales móviles registrados con la VPN con un número de código que corresponde al número de extensión usado por la organización para la cual se proporciona la VPN, el usuario de un terminal móvil puede hacer y recibir llamadas como si fuera una extensión fija estándar para la centralita de la organización. El MSISDN "convencional" también se puede usar para hacer y recibir llamadas desde el terminal móvil.

Además de o alternativamente a simplificar la marcación de números entre terminales móviles dentro de la VPN, miembros de la VPN se pueden dotar por la red de telecomunicaciones móviles con tarifas de llamada especiales entre miembros de la VPN. Se pueden proporcionar facilidades especiales a miembros de la VPN – por ejemplo, facturación centralizada a la organización, más que la emisión de facturas separadas a cada abonado en la VPN.

Los elementos de las dos redes de telecomunicaciones móviles y su operación, se describirán ahora brevemente con referencia a la Figura 1.

Cada estación base (BS) corresponde a una celda respectiva de su red de telecomunicaciones y recibe llamadas desde y transmite llamadas a un terminal móvil en esa celda mediante comunicación radio inalámbrica. Tal terminal

móvil de abonado se muestra en 1A. Las estaciones base se disponen en grupos y cada grupo de estaciones base se controla por un centro de conmutación móvil (MSC), tal como el MSC 2A para las estaciones base 3A, 4A y 5A. Como se muestra en la Figura 1, la red A tiene otro MSC 6A, que está controlando tres estaciones base adicionales 7A, 8A y 9A. En la práctica, la red A incorporará muchos más MSC y estaciones base que los mostrados en la Figura 1.

Cada abonado a la red se dota con una tarjeta inteligente o SIM que, cuando se asocia con el terminal móvil del usuario identifica el abonado a la red. La tarjeta SIM está preprogramada con un número de identificación único, la "Identidad de Abonado Móvil Internacional" (IMSI) que no es visible en la tarjeta y no es conocida por el abonado. El abonado se pone en circulación con un número conocido públicamente, es decir, el número de teléfono de abonado, por medio del cual se inician las llamadas al abonado por las personas que llaman. Este número es el MSISDN. Además, el terminal móvil 1A es un miembro de una VPN y también puede tener un número de código, como se describió anteriormente.

La red incluye un registro de localización de abonado (HLR) 10A que, para cada abonado a la red, almacena la IMSI y el MSISDN juntos con otros datos de abonado.

Cuando el abonado desea activar su terminal móvil en una red (de manera que pueda hacer o recibir llamadas posteriormente), el abonado coloca su tarjeta SIM en un lector de tarjeta asociado con el terminal móvil (terminal 1A en este ejemplo). El terminal móvil 1A entonces transmite la IMSI (leída de la tarjeta) a la estación base 3A asociada con la celda particular en la que está situado el terminal 1A. La estación base 3A entonces transmite esta IMSI al MSC 2A con el cual está registrada la BS 3A.

El MSC 2A ahora accede a la ubicación adecuada en el HLR 10A presente en el núcleo de la red 12A y extrae el MSISDN de abonado correspondiente y otros datos de abonado desde la ubicación de almacenamiento adecuada y los almacena temporalmente en una ubicación en un registro de localización de visitante (VLR) 14A. De este modo, por lo tanto el abonado particular se registra eficazmente con un MSC particular (MSC 2A) y la información del abonado se almacena temporalmente en el VLR (VLR 14A) asociado con ese MSC.

Cada uno de los MSC de la red (MSC 2A y MSC 6A) tiene un VLR respectivo (14A y 11A) asociado con él y opera del mismo modo que ya se describió cuando un abonado activa un terminal móvil en una de las celdas correspondientes a una de las estaciones base controladas por ese MSC.

Cuando el abonado que usa el terminal móvil 1A desea hacer una llamada, habiendo insertado ya la tarjeta SIM en el lector asociado con este terminal móvil de la manera descrita, se puede hacer una llamada introduciendo el número de teléfono de la parte llamada de la forma usual. Esta información se recibe por la estación base 3A y entonces se encamina a la parte llamada a través del MSC 2A. Por medio de la información mantenida en el VLR 14A, el MSC 6A puede asociar la llamada con un abonado particular y de esta manera registrar información para propósitos de tarificación.

De manera similar, cuando una parte que llama (ya sea un abonado dentro de la red A o fuera de ella) hace una llamada para el abonado usando el terminal móvil 1A, el MSC 2A es capaz de encaminar esta llamada al terminal móvil 1A a través de la estación base 3A usando la información relacionada con ese abonado que está almacenada temporalmente en el VLR 14A.

Lo precedente se destina a ser meramente una descripción simplificada de la operación normal de la red GSM. En la práctica, se llevarán a cabo otros procedimientos. En particular, tendrá lugar un procedimiento de autenticación cuando un abonado activa un terminal móvil usando su SIM.

También mostrado en la Figura 1 está una segunda red GSM B. Los elementos en la red B que corresponden a aquéllos en la red A son referenciados de manera similar, pero con el sufijo "B" en lugar de "A". Por supuesto, la red "B" es probable que tenga una diferente disposición y número de MSC y estaciones base pero opera de una manera similar a la red A.

Como se explicó anteriormente, para un abonado a la red A, la IMSI respectiva y el MSISDN y otros datos relevantes particulares a ese abonado se almacenarán en el HLR 10A. Si ese abonado ahora transita a la red B y activa un móvil tal como la MS 1B en esa red, se repite sustancialmente el procedimiento descrito anteriormente.

Por lo tanto, el abonado inserta su tarjeta SIM en el lector de tarjeta del terminal móvil 1B. El terminal móvil 1B entonces transmite la IMSI desde la tarjeta a la estación base adyacente (3B) y de allí al MSC 2B.

No obstante, el MSC 2B reconocerá ahora, a partir de la estructura de la IMSI, que el abonado no es un abonado a la red B sino un abonado a la red A. Por lo tanto, el MSC 2B accederá, a través del núcleo 12B, al HLR 10A en lugar de al HLR 10B usando la interconexión 16 entre la red A y la red B. La información de abonado, que incluye el MSISDN relevante y otros datos de abonado, se accederá y almacenará temporalmente en el VLR 14B. Toda esta información está lista por lo tanto para uso en el procesamiento de llamadas a o desde el terminal móvil 1B. Cualquier información de tarificación asociada con cualquier llamada tal entonces se puede asociar con la

información de abonado en el VLR 14B y transmitir eventualmente de vuelta al HLR 10A y entonces facturar al abonado relevante.

Si una parte que llama desea hacer una llamada a un abonado visitante que está usando el terminal móvil 1B, la llamada se encaminaría inicialmente a la red A (debido a que esta red sería la red identificada por el número de teléfono conocido públicamente del abonado que usaría la parte que llama). El núcleo 12A interrogaría al HLR 10A lo que produciría por lo tanto una indicación de que una copia de los datos del abonado se almacenó temporalmente en el VLR 14B, indicando, por supuesto, que el abonado ha transitado a la red B. A través del enlace 16 entre las redes A y B, la red A interroga a la red B para pedir un “número de tránsito”. Este es, en efecto, un número de teléfono temporal para el abonado, que es un número adecuado para la red B. Este número de tránsito se puede usar ahora para encaminar la llamada de la parte que llama a la red B y de allí al terminal móvil 1B. La parte que llama no sería consciente por supuesto de este número de tránsito o del proceso de transferencia.

La descripción precedente es meramente una descripción simplificada de la operación normal de la red GSM y el tránsito entre redes GSM. Detalles adicionales de todos los aspectos de las redes GSM y el tránsito están disponibles en la documentación de los Estándares del ETSI.

Como se trató anteriormente, además del encaminamiento de llamadas usando un MSISDN convencional, también es conocido permitir a abonados seleccionados de una red de telecomunicaciones móviles formar una VPN entre ellos. El núcleo 12A de la red A incluye un nodo inteligente (IN) 18 que almacena la base de datos de números de código asociados con los MSISDN respectivos. Es decir, el IN 18 comprende una tabla de búsqueda o base de datos, que permite que sea identificado el MSISDN adecuado que corresponde a un número de código particular y viceversa.

Si el usuario del terminal móvil 1A (que es un miembro de una VPN (VPN X)) administrado por el núcleo 12A de la red A desea llamar a otro miembro de esa VPN, el usuario marca el número de código de ese otro terminal móvil. En este caso, el terminal móvil llamado es el terminal móvil 20. El terminal móvil 20 es un miembro de la VPN X y tiene su MSISDN almacenado en el IN 18 junto a ese número de código del terminal móvil (“4573” en este ejemplo). Debido a que el terminal móvil 20 está en la misma VPN que el terminal móvil 1A, el usuario del terminal móvil 1A necesita marcar solamente el número de código del terminal móvil 20.

Los intercambios de datos que tienen lugar durante la iniciación de tal llamada se muestran en la Figura 2. Un mensaje de iniciación de llamada 1, que incluirá el número de código marcado por el usuario del terminal móvil 1A, se transmite inalámbricamente desde el terminal móvil 1A al MSC 2A. El mensaje de iniciación entonces se transmite desde el MSC 2A al núcleo 12A, típicamente mediante una conexión cableada o fija (mensaje 2). El mensaje de iniciación incluye una marca u otro identificador que indica que la llamada que se inicia es para una llamada dentro de una VPN particular (VPN X). Esta marca se identifica por el núcleo 12A. En la identificación de la marca, el núcleo 12A transmite el número de código extraído a partir del mensaje de iniciación al IN 18 (mensaje 3). El IN 18 entonces consulta la tabla de búsqueda o base de datos presente en el mismo y obtiene el MSISDN que corresponde al número de código – en este ejemplo, “077712254573”. El MSISDN se devuelve al núcleo 12A (mensaje 4) y se transmite desde el núcleo 12A al MSC 2A (mensaje 5). El MSC 2A entonces modifica el mensaje de iniciación de llamada para incluir el MSISDN del terminal móvil llamado 20 en lugar del número de código. El mensaje de iniciación de llamada modificado entonces se transmite al núcleo 12A (mensaje 6), donde se maneja de una manera similar a cualquier otra llamada de teléfono marcada usando un MSISDN convencional. No obstante, la marca que indica que la llamada es entre miembros de la VPN X se usa por el núcleo 12A para identificar y poner a disposición cualquier servicio especial que se ha acordado por la red que se proporcionará a los miembros de la VPN X y también para tarificar la llamada según la estructura de tarificación acordada para los miembros de la VPN X. El mensaje de iniciación de llamada modificado entonces se transmite desde el núcleo 12A al MSC 6A conectado a la BS 7A que sirve al terminal móvil 20 (mensaje 7). El mensaje de iniciación de llamada entonces se pasa por el MSC 7A al terminal móvil 20 (mensaje 8), después de lo cual la llamada de teléfono entre los teléfonos móviles 1A y 20 puede proceder de la manera convencional.

Si el terminal móvil 20 está transitando en la red B y por lo tanto es servido por la estación base 7B, el MSC 6B y el VLR 11B (Figura 1), aún puede ser posible para la llamada ser encaminada al terminal móvil 20 marcando el número de código en el terminal 1A. Ese terminal móvil 20 que está transitando en la red B se graba en el HLR 10A de la manera descrita anteriormente. La Figura 3 muestra los mensajes intercambiados entre los elementos mostrados en la Figura 1 durante la iniciación de llamada. Los mensajes 1 a 6 son los mismos que esos mensajes descritos en relación con la Figura 2.

Cuando el mensaje 6, que inicia la llamada entre el terminal móvil 1A y el terminal móvil 20 se recibe por el núcleo 12A y el HLR 10A se consulta, el HLR 10A indicará que una copia de los datos relativos al usuario del terminal móvil 20A se almacenó temporalmente en el VLR 11B asociado con el MSC 6B que controla la estación base 3B con la cual está registrado el terminal móvil 20B en la red B. El núcleo 12A de la red A entonces transmite el mensaje de iniciación de llamada al núcleo 12B de la red B a través de la interconexión 16 (mensaje 10). El mensaje entonces se encamina al MSC adecuado (MSC 6B) (mensaje 11) y de allí al terminal móvil 20 (mensaje 12). Cuando la llamada se acepta por el terminal móvil 20, la comunicación entre el terminal móvil 1A y el terminal móvil 20 puede ocurrir de

la manera convencional. Aunque la llamada es entre miembros de la VPN X, la tarificación por hacer la llamada puede ser más alta para reflejar que el terminal móvil 20 está transitando.

La Figura 4 muestra el procedimiento de iniciación de llamada cuando se inicia una llamada transitando el terminal móvil 20 a otro miembro de la VPN X.

El mensaje de iniciación de llamada (mensaje 20) incluye el número de código del terminal dentro de la VPN que se llama – por ejemplo, el terminal móvil 1A. El mensaje de iniciación de llamada se recibe desde el terminal móvil 20 por el MSC 6B (a través de un enlace inalámbrico) y entonces se transmite (a través de un enlace fijo o cableado) al núcleo 12B (mensaje 21). Como se indicó anteriormente, el mensaje de iniciación de llamada incluye una marca que indica que el mensaje es un mensaje para establecer una llamada desde un miembro de la VPN X a otro miembro de la VPN X. Esta marca es reconocida por el núcleo 12B, donde también se determina que la VPN X se administra por la red A. El núcleo 12B entonces extrae el número de código a partir del mensaje de iniciación de llamada y envía este al núcleo 12A de la red A a través de la interconexión 16 (mensaje 22). El número de código se recibe por el núcleo 12A, que consulta el IN 18 para determinar a partir de la tabla de búsqueda almacenada en el mismo el MSISDN que corresponde al código corto (mensaje 23). El MSISDN que corresponde al código corto entonces se transmite desde el IN 18 al núcleo 12A (mensaje 24). El núcleo 12A entonces transmite el MSISDN al núcleo 12B a través de la interconexión 16 (mensaje 25). El núcleo 12B entonces modifica el mensaje de iniciación de llamada sustituyendo el número de código con el MSISDN proporcionado en el IN 18 y envía este al MSC 6B (mensaje 26). El procedimiento de iniciación de llamada entonces puede continuar como para una llamada convencional (y no se describirá aún más aquí por el bien de la brevedad).

En esta especificación, los MSISDN se contemplan como que están almacenados en el IN 18. No obstante, se debería entender que cualquier tipo de número de teléfono (o dirección de dispositivo) se puede almacenar y usar para sustituir un número de código correspondiente. Por ejemplo, el número de teléfono puede ser un número de teléfono de PSTN fijo. Las referencias en esta especificación a un MSISDN se deberían interpretar también que son referencias a cualquier tipo de número de teléfono o dirección de dispositivo.

La Figura 5 muestra un ejemplo de los datos almacenados por el IN 18. El IN 18 almacena detalles de los números de código y MSISDN o números de teléfono para dos VPN: la VPN X y la VPN Y. Por supuesto, en la práctica, el IN 18 podría almacenar datos para una multiplicidad de VPN. Para cada número de código de una VPN particular el IN 18 almacena el MSISDN correspondiente. Varios números de código pueden corresponder a un MSISDN único (es decir, si un abonado marca dos números de código diferentes, se devolverá el mismo MSISDN).

Por ejemplo, para la VPN X el número de código “0” corresponde al MSISDN (número de teléfono de PSTN) “0207 225 1000”. Este podría ser, por ejemplo, el número de teléfono de PSTN de la centralita de la organización para el cual se proporciona la VPN X. Otros números de código (4573…. 4965) corresponden a MSISDN respectivos (07771 225 4573…07771 225 4965). Otros números de código (4990, 4491) corresponden a números de teléfono de PSTN de otro país (en este ejemplo Alemania).

El IN 18 también enumera números de código y los MSISDN correspondientes para la VPN Y. Los números de código en la VPN Y tienen una longitud diferente a los números de código de la VPN X. Es ventajoso para la organización para la que se proporciona la VPN usar sus números de extensión existentes (por ejemplo, usados para hacer llamadas internas dentro de la red de telefonía fija de la organización) como los números de código sin modificación.

Como se indicó anteriormente, el mensaje de iniciación de llamada desde un terminal móvil que es miembro de una VPN incluirá una marca u otro identificador que indica de qué VPN es miembro el terminal. Además del número de código que se reenvía por el núcleo 12A al IN 18, también se reenvía esta marca u otro identificador. Esto permite al IN 18 identificar inicialmente la VPN relevante y, posteriormente, usar el número de código, para obtener el MSISDN relevante (u otro número de teléfono).

Se debería apreciar que, aunque los ejemplos dados anteriormente de la técnica anterior y las realizaciones de la invención descritas más adelante, conciernen a sistemas de telecomunicaciones móviles GSM, la presente invención es aplicable a cualquier tipo de sistema de telecomunicaciones móviles o celulares, incluyendo un sistema de telecomunicaciones móviles UMTS (3G).

Como se describió anteriormente, la disposición de VPN conocida puede encaminar con éxito llamadas entre miembros de una VPN cuando esos miembros están transitando en una red de telecomunicaciones móviles (que no está alojando la VPN). No obstante, en la disposición de la técnica anterior, no es posible encaminar llamadas marcadas usando números de código entre miembros de las VPN alojadas o administradas por diferentes redes. Tampoco es posible en la disposición de la técnica anterior proporcionar una única VPN que incluya miembros de una pluralidad de redes. Tales redes “diferentes” pueden tener núcleos de red separados, que controlan la autenticación de los abonados y la tarificación para uso de la red relevante por los abonados. Las diferentes redes se pueden controlar y operar completamente independientemente unas de otras y pueden ser entidades legales diferentes. Alternativamente, diferentes redes pueden ser poseídas en común pero pueden estar situadas en diferentes países o regiones, cada red que tiene un núcleo respectivo para controlar la operación total de esa red.

La realización a ser descrita permite que los datos de las VPN o planes de marcación privados alojados por diferentes redes de telecomunicaciones móviles sean compartidos. Las redes seleccionadas pueden acordar en principio permitir la compartición de datos de las VPN alojadas por las mismas. Cuando tal disposición está en su lugar en principio, cada red especificará y solamente permitirá la compartición de, las VPN seleccionadas alojadas por la misma. Además, puede haber algunas entradas de una VPN que no van a ser compartidas entre las redes. El IN de cada red controla con qué (en su caso) otras redes se comparten los datos de la VPN. Mediante la compartición de datos de las VPN alojadas o administradas por diferentes redes, un abonado registrado con una VPN alojada por la red A puede marcar a un abonado de una VPN diferente, alojado por la red B, usando el código corto del abonado de la VPN alojado por la red B. Tal disposición es particularmente ventajosa, por ejemplo, cuando una organización multinacional, que tiene VPN en varios países diferentes y alojadas por diferentes redes (que podrían ser quizás poseídas en común) desea dotar a sus empleados con la facilidad de usar números de código para hacer llamadas internacionalmente pero dentro de la organización. Además o alternativamente, se pueden proporcionar servicios especiales y tarificación de llamada para tales llamadas entre VPN.

La realización también permite a una VPN única abarcar una pluralidad de redes. Es decir, los miembros de una única VPN pueden ser abonados de diferentes redes.

La Figura 6 muestra las dos redes GSM de la Figura 1, modificadas según una realización de la invención. En la Figura 6, a modo de ilustración, existe un acuerdo entre las redes A y B para compartir datos de todas las VPN alojadas por cada una de las dos redes. Además de los componentes mostrados en la Figura 1, la Figura 6 incluye además un sistema de Mediación y Suministro de VPN Internacional (sistema IMP) 30. El sistema IMP 30 mantiene una base de datos 32 de números de código y los MSISDN correspondientes (E 164 miembros que se pueden marcar y/u otros números de teléfono o direcciones de dispositivo) del IN 18A y el IN 18B de las redes A y B – es decir los datos de VPN almacenados por cada una de las redes. Cada una de las redes A y B se dota con un adaptador de suministro IMP 34A, 34B, que proporciona una interfaz entre el IN 18A, 18B de las redes A y B y el sistema IMP 30.

El sistema IMP 30 almacena una copia de los datos del número de código y el MSISDN (y/u otros números de teléfono o direcciones de dispositivo) almacenados en el IN 18A, 18B de cada red servida por el sistema IMP 30. Los datos se almacenan en la base de datos 32 en un formato predeterminado como un fichero XML. El formato de los datos almacenados en el IN local 18A, 18B de cada red puede ser diferente de este formato predeterminado. El adaptador 34A, 34B de cada red local modifica los datos almacenados en el IN 18A, 18B de cada red para ponerlos en el formato estándar predeterminado, anterior a que los datos sean transmitidos al sistema IMP 30 y desde allí a la base de datos 32.

Hablando en términos generales, el sistema IMP 30 y la base de datos 32 permitirán a un abonado a una red (red A) llamar a un abonado de otra red (red B) usando un número de código del abonado de la red B con respecto a una VPN alojada por el IN 18B de la red B. Cuando el número de código se marca por el abonado de la red A, el mensaje de iniciación de llamada se pasa desde el terminal móvil 1A a través de la estación base 3A al MSC 2A y desde allí al núcleo de red 12A. El número de código se reconoce como que no es un MSISDN y se pasa al IN 18A. El IN 18A a su vez reconoce que el número de código no es para una VPN que el aloja. Lo que ocurre a continuación depende de la implementación del sistema IMP 30.

En una primera implementación el IN 18A genera una petición del MSISDN correspondiente al número de código y envía este a su adaptador 34A. El adaptador 34A configura esta petición en el formato XML requerido y transmite este al sistema IMP 30. El sistema IMP 30 interroga la base de datos 32 para proporcionar el MSISDN correspondiente al número de código y devuelve este al IN 18A a través del adaptador 34A. El IN 18A entonces devuelve el MSISDN al MSC 2A a fin de permitir a la llamada continuar de la manera convencional.

En una segunda disposición, preferida, los números de código y los MSISDN de todas las VPN alojadas por otras redes (red B en este ejemplo) con las cuales la red A desea permitir marcar usando los números de código se copian al IN 18A de la red A. Si se usa tal disposición, el IN 18A será capaz de buscar el MSISDN relevante para un número de código de una VPN que no está alojada en el IN 18A usando la información descargada, sin requerir una consulta al sistema IMP 30 y la base de datos 32 a través del adaptador 34A. Por supuesto, además de la red A que recibe una copia de todos los números de código y los MSISDN para las VPN relevantes alojadas por las otras redes, esas otras redes (red B en este ejemplo) también requerirán copias de los detalles relevantes de las VPN relevantes que no alojan ellas (las VPN de la red A en este ejemplo). En este caso, las redes de alojamiento de las VPN siguen siendo el almacén de datos maestro para sus propios datos de VPN.

Cualquiera de las dos disposiciones que se use, se pueden proporcionar servicios especiales para y se pueden aplicar tarificaciones especiales a, llamadas entre las VPN alojadas por diferentes redes, siendo diferentes estos de los servicios y tarificaciones prestados por las llamadas marcadas convencionalmente usando los MSISDN. Si una llamada es entre terminales de abonado servidos por las VPN que tienen una asociación (es decir, las VPN entre las cuales existe un acuerdo para permitir que las llamadas sean encaminadas entre las mismas usando sus números de código o entre las cuales existe un acuerdo para unir las VPN en una asociación, con o sin números de código), tales llamadas se denominan llamadas “en línea”. Las llamadas que no usan los números de código y que no son

entre terminales de abonado de las VPN asociadas se denominan “fuera de línea”. Tales llamadas fuera de línea son llamadas convencionales entre abonados de la red de telefonía móvil o entre un abonado de telefonía móvil y un abonado a una red fija. Se puede ofrecer una tarifa y servicios diferentes a un terminal de abonado que hace una llamada en línea dependiendo de si esa llamada es entre terminales de abonado que son miembros de la misma VPN y donde ambos terminales de abonado están en su red doméstica. Pueden estar disponibles una tarificación y servicios diferentes cuando los terminales de abonado son ambos miembros de la misma VPN pero uno de los abonados está transitando dentro una red visitada. De nuevo se puede proporcionar una estructura de tarificación y servicios diferente cuando una llamada es entre dos terminales de abonado que son miembros de diferentes VPN y además pueden variar en dependencia de si las VPN diferentes se alojan por la misma red o diferentes redes y de la ubicación de los terminales de abonado respectivos entre los cuales se hace la llamada.

A fin de que la base de datos 32 sea compilada, el IN 18A, 18B de cada red debe proporcionar sus contenidos a la base de datos 32. Como se indicó anteriormente, los adaptadores de suministro 34A, 34B son operables para disponer los datos de cada VPN alojada en una forma predeterminada XML adecuada y está se pasa a la base de datos 32. La base de datos 32 se actualizará regularmente con incorporaciones, eliminaciones y enmiendas a las VPN alojadas en cada IN 18A, 18B. Si la segunda disposición descrita anteriormente aplica, también se actualizarán periódicamente las copias de las bases de datos de VPN descargadas a cada IN 18A, 18B desde la base de datos 32.

Como se describió anteriormente en relación con la disposición convencional donde una red de telecomunicaciones móviles proporciona las VPN para una pluralidad de organizaciones, es necesario que el IN 18A pueda distinguir entre números de código para las VPN respectivas alojadas por el mismo.

En la realización descrita las redes A y B están situadas en diferentes países. Una disposición conveniente para distinguir códigos cortos de las VPN asociadas con la red A de aquellas asociadas con la red B es añadir automáticamente a los códigos cortos un prefijo de unicidad (tal como el código de marcación de país estándar para el país donde se aloja la VPN) cuando el código corto se prepara en el adaptador 34A, 34B para transmisión al sistema IMP 30. Por lo tanto, los números de código de las VPN alojadas por la red A, que se sitúan en el Reino Unido, todos tendrían añadido a ellos el prefijo “44” por el adaptador 34A anterior a que sean transmitidos al sistema IMP 30. Los códigos cortos de las VPN alojadas por la red B, que está situada en Alemania, tendrían automáticamente el prefijo “49” añadido a ellos por el adaptador 34B anterior a que sean transmitidos al sistema IMP 30. El prefijo de unicidad (código de país) está además del prefijo opcional que identifica de manera única cada número de código como un miembro de su VPN dentro de la red que aloja la VPN (si se usa tal prefijo).

En la discusión en lo sucesivo, se describirá una implementación de la segunda disposición a la que se refiere anteriormente, donde el IN de cada red mantiene una copia de los datos de VPN de cada una de las VPN asociadas alojadas por otras redes. Los datos de la VPN se “empujan” desde cada IN (IN 18A e IN 18B) al sistema IMP 30 de dos formas primarias. Los datos se pueden empujar selectivamente. Por ejemplo, cuando un nuevo miembro se une a una VPN alojada por la red A, la información relevante (código corto, MSISDN, código de país e identificador de VPN) se empujan al sistema IMP 30. Un modo de actualización alternativo es donde el contenido entero del IN o de una VPN particular alojada por el IN, se empuja al sistema IMP 30. Este modo se usará cuando se configura inicialmente el sistema IMP 30 (debido a que no tendrá registro de ninguna entrada del IN de la red A). Este modo se puede usar posteriormente para realizar una reconciliación de los datos almacenados por el IN de la red A y los datos para la red A almacenados por el sistema IMP 30. Si hay cualquier discrepancia entre los datos estos se pueden identificar y resolver.

El IN de cada red también necesitará “arrastrar” los datos relacionados con las VPN alojadas por otras redes desde el sistema IMP 30. De nuevo, este arrastre de datos se puede realizar o bien selectivamente o bien se pueden descargar todos los datos mantenidos para una VPN o IN particular (o una parte de esos datos) – este último modo que se usa típicamente durante el ajuste del sistema y para realizar una operación de reconciliación del tipo descrito anteriormente en relación a un dato empujado por un IN.

La base de datos 32 es una base de datos relacional e incluye datos de suministro relevantes para todas las VPN. La base de datos almacena un número de código correspondiente, número de teléfono (o similar), identificador de VPN y código de país para cada entrada.

La Figura 9 muestra un ejemplo de los datos almacenados en la base de datos 32. La Figura 10 muestra un ejemplo de los datos correspondientes arrastrados por el IN 18A de la red A.

Además de almacenar los números de código, los números de teléfono, etc., la base de datos 32 también almacena datos que indican cuándo se actualizaron por última vez las entradas en la misma y cuándo los datos de la base de datos 32 han actualizado por última vez la información correspondiente almacenada en el IN de cada red relevante. Esta información se puede usar para permitir la actualización selectiva de los datos almacenados en el IN de cada red relevante.

El adaptador de suministro 34A, 34B de cada red es responsable de todas las comunicaciones entre el IN 18A, 18B de esa red y el sistema IMP 30. El adaptador de suministro es una aplicación Java única. El adaptador de suministro

incluye un programador que desencadena las operaciones de arrastre y empuje según una programación preprogramada y configurable. Además de permitir las operaciones de arrastre y empuje, como se describió anteriormente, el adaptador de suministro también realiza una operación de archivo, donde el adaptador de suministro mueve periódicamente los datos almacenados en el IN a un almacén de archivos donde se almacenan los datos de forma comprimida.

Los adaptadores de suministro comunican con un sistema central 30 intercambiando ficheros formateados XML. El protocolo de transporte de ficheros es SCP (Protocolo de Copia Segura). Este protocolo usa el cifrado y la autenticación de intérprete de órdenes seguro (SSH). El intérprete de órdenes seguro es un estándar industrial para establecimiento y mantenimiento de conexiones seguras. Usa algoritmos DES y RSA para gestión de claves públicas/privadas. Los datos transferidos se cifran y protegen de manipulación. La protección de tunelización de intérprete de órdenes seguro es equivalente al proporcionado por una red privada virtual IP. El intérprete de órdenes seguro usa encaminamiento IP estándar y también puede ejecutarse dentro de una red privada virtual IP. Todas las operaciones de transferencia de ficheros se inician por los adaptadores 34A, 34B.

El túnel se establece solamente durante el tiempo necesario para realizar las operaciones de arrastre, empuje o archivo. Después de que se completen estas operaciones, el túnel se desmantela. Esto permite al sistema operar usando, por ejemplo, conexiones de ISDN, que se establecen solamente cuando se necesitan. El servidor SSH tiene un certificado de anfitrión que debe coincidir con la entrada relevante en el sistema IMP 30 que almacena detalles de cada adaptador 34A, 34B conocido. El sistema IMP 30 almacena una clave pública asociada con cada adaptador 34A, 34B para autorizar acceso. Cada adaptador 34A, 34B usará su propia clave privada para acceder al sistema IMP 30. Cada adaptador almacenará un certificado de anfitrión del sistema IMP 30 en su lista de “anfitriones conocidos”.

Como medida de seguridad, el sistema IMP se puede configurar de manera que solamente permitirá a un IN 18A arrastrar datos desde la base de datos 32 si ese IN 18A tiene datos empujados previamente.

Como se muestra en la Figura 7 el sistema IMP 30 se dota con una interfaz gráfica de usuario (GUI) 36 para monitorizar la operación del sistema IMP 30, analizar fallos y conexión manual a los adaptadores 34A, 34B.

Con referencia a la Figura 7, se describirá ahora un ejemplo de los flujos de datos cuando la red A carga datos al sistema IMP 30 y la red B descarga datos.

Flujo de datos 1: La red A, por medio del IN 18A, proporciona datos de VPN de sus abonados al adaptador 18A. La red A especifica las operaciones de actualización (añadir o modificar) y eliminación a llevar a cabo en los datos almacenados por el sistema IMP 30. La actualización puede ser o bien una actualización selectiva (diferencial) o bien una reconciliación completa o parcial de datos que conciernen a la VPN.

Flujo de datos 2: El adaptador 34A carga los datos al sistema IMP 30. El adaptador 34A realiza toda la comunicación y manipulación de errores con el sistema IMP 30.

El sistema IMP 30 comprobará que cada número de código y MSISDN recibido es válido. Esto se puede hacer por un camino de comunicación separado para la red relevante que aloja el número de código y el MSISDN. La base de datos 32 solamente se actualizará (ver el flujo de datos 3 más adelante) con números de código y MSISDN válidos. Para cualquier número de código y MSISDN que no es válido, se producirá un informe y devolverá al adaptador 34A (flujo de datos 4 más adelante).

Flujo de datos 3: El sistema IMP 30 actualiza su base de datos 32 según los datos recibidos desde la red A.

Flujo de datos 4: El sistema IMP 30 devuelve al adaptador 34A un informe del éxito o fallo de cada operación de actualización.

Cuando la red B desea descargar datos de VPN, ocurren los siguientes flujos de datos.

Flujo de datos 5: La red B, por medio de su IN 18B, solicita desde su adaptador 34B una descarga de algunos datos de suministro especificados relativos a las VPN de otras redes. Tales peticiones se pueden programar periódicamente o desencadenar manualmente por un operador. Las peticiones pueden ser o bien para una actualización selectiva/diferencial o bien para una reconciliación completa o parcial.

Flujo de datos 6: El adaptador 34B determina las VPN de otras redes con las que la red B tiene una asociación (es decir entre las que se pueden hacer llamadas entre VPN o en red) y para las cuales se deberían descargar datos de suministro relevantes.

Flujo de datos 7: El adaptador 34B inicia una descarga desde el sistema IMP 30, especificando una lista de VPN desde las cuales se requieren datos. El adaptador 34B realiza toda la comunicación y manejo de errores con el sistema IMP 30.

Flujo de datos 8: El sistema IMP recupera los datos relevantes para las VPN de su base de datos 32. Los datos

incluyen números de código, números de teléfono para las entradas de todas las VPN relevantes excepto para las VPN alojadas por la red B.

Flujo de datos 9: El sistema IMP 30 devuelve los datos solicitados al adaptador 34B.

Flujo de datos 10: El adaptador 34B devuelve los datos solicitados desde las VPN de otras redes al IMP de la red B.

La GUI 36 permite que el servicio VPN entre redes 30 sea gestionado como sigue.

Flujo de datos 11: El sistema GUI 36 puede añadir, actualizar y eliminar datos de configuración del sistema IMP 30, tales como redes participantes válidas y cuentas de VPN.

Flujo de datos 12: El sistema GUI 36 puede corregir datos en la base de datos del sistema IMP 30.

Flujo de datos 13: El sistema GUI 36 puede generar informes a partir de la base de datos del sistema IMP 30.

La arquitectura del sistema IMP 30 se muestra en la Figura 8. El módulo de proceso despachador 40 es responsable de la decodificación de las peticiones XML o ficheros cargados recibidos desde el adaptador de una red (en este ejemplo el adaptador 34A de la red A). El proceso despachador 40 también actualiza la base de datos 32 según los ficheros cargados recibidos y prepara los ficheros devueltos XML para enviarlos al adaptador 34A.

El módulo de mantenimiento (archivo) 42 es responsable de archivar y purgar los ficheros XML viejos u obsoletos y purgar entradas sobrantes de un almacén de operaciones de arrastre y empuje pasadas.

El servidor de registro 44 es responsable de escribir las entradas de registro generadas por todos los componentes del sistema IMP 30 a los ficheros de registro.

El servidor de aplicaciones 46 del sistema GUI 36 proporciona acceso a la base de datos y lógica de negocio asociada y hojas de estilo XML. El servidor web 48 y el navegador web 50 proporcionan un medio conveniente para implementar la interfaz gráfica de usuario a partir del sistema GUI 36. El sistema de ficheros 52 gestiona las peticiones de arrastre y empuje desde el adaptador 34A.

Lo siguiente es un resumen de gestión de empuje/arrastre de información entre las redes y el sistema IMP 30:

- La IMP funciona con un mecanismo de empuje y arrastre.
- Las redes empujan sus propios números al IMP, formateados con el prefijo de unicidad global y asignados a una cuenta de cliente (una VPN particular).
- Las redes arrastran los números para las cuentas de cliente que poseen.

  Las redes no pueden arrastrar los números para cuentas de cliente a las que no están asignadas.
- Las redes pueden empujar o arrastrar grupos de números seleccionados:
  - Números que pertenecen a una o más cuentas de cliente
  - Números que pertenecen a una o más redes
- Son posibles diversas acciones de empuje/arrastre:
  - Actualización de empuje (añadir o sustituir un número)
  - Arrastre (recuperar un número empujado por otra red)
  - Borrar un número
  - Arrastre de reconciliación (la red puede arrastrar todos o un subconjunto de todos los datos que se han empujado previamente al IMP, a fin de verificarlos)
  - Empuje de reconciliación (la red empuja datos a la IMP, que borra o sustituye todos los datos empujados previamente por la red para una cuenta de cliente particular.

Con referencia ahora a la Figura 10, el contenido del IN 18A de la red A se muestra después de que el IN 18A ha arrastrado datos relevantes desde dos VPN (la VPN M_B y la VPN N_B desde otra red (red B) con la que hay un acuerdo para permitir llamar en red entre VPN. Los números de código de la VPN M_B incluyen un identificador de VPN único “2” y, en este caso, el código de país “49” (que se refiere al país (Alemania) donde se aloja la VPN). Estos dígitos preceden el número de código básico “12340….12347”. De manera similar, los números de código de la VPN N_B tienen un identificador de VPN único “4” y el código de país “49” que precede el número de código básico relevante “1…8”. Como se trató anteriormente, el identificador de VPN “único” es único dentro de esa red de

alojamiento de la VPN, pero se podría repetir en otra red.

Los números de códigos de la VPN X y la VPN Y, que están alojadas en la red A (y en la Figura 10 se designan VPN X_A y VPN Y_A) se pueden considerar que son VPN "locales". Estas no habrán añadido a ellas un identificador de VPN único o un código de país. Cuando los datos de la VPN X_A e Y_A se cargan al sistema IMP 30, el adaptador 34A añadirá un identificador de VPN único relevante y código de país a fin de poner los datos de VPN en el formato requerido para el sistema IMP 30.

Se debería entender que cualquier red puede alojar las VPN que solamente se requieren localmente dentro de esa red y donde los detalles de las cuales nunca se pasan al sistema IMP 30.

Debido a que los números de código de las VPN locales (la VPN X_A y la VPN Y_A no se procesan por el adaptador 34A y el sistema IMP 30 y no se dotan con un identificador de VPN único y código de país, es posible que un número de código usado por una VPN local sea el mismo que el número de código usado en los datos de VPN arrastrados. En la Figura 10 la última entrada de la columna de la izquierda para la VPN X_A tiene un número de código "4491". El primer número de código de la VPN N_B es también "4491", aunque este último número de código comprende un identificador de VPN único "4", código de país "49" y número de código básico "1".

Tal situación puede ser tratada en una variedad de formas diferentes. El IN 18A puede monitorizar cualquier conflicto entre los números de código de diferentes VPN y producir un informe que sugiere intervención manual. Por ejemplo, se podría enviar un mensaje a la red B y en particular a la persona responsable de administrar la VPN N_B que indica que el abonado con el número de código básico "1" de la VPN N_B debe cambiar ese número de código o no serán capaces de acceder a la VPN N_B cuando se transita en la red A. Si el conflicto no se resuelve, el IN 18A de la red A asumirá, a la recepción del número de código "4491" en un mensaje de iniciación de llamada, que este es el número de código de la VPN X_A local y devolverá el número de teléfono +49 89 2399 4991".

La Figura 9 muestra los datos presentes en la base de datos 32 del sistema IMP que sigue al empuje de datos para la VPN X_A e Y_A desde la red A y desde la VPN M_B y la VPN N_B desde la red B. El conflicto entre los números de código descritos en relación a la Figura 10 no ocurre debido a que el número de código "4491" de la VPN X_A ha añadido a él el identificador de VPN único "1" y el código de país "44".

La base de datos 32 no obstante monitoriza los conflictos de los números de código cuando los datos de la VPN están siendo empujados desde una red. Si la base de datos 32 detecta un conflicto entre los números de código o MSISDN dentro de una asociación de VPN, este se notifica usando la GUI 36 y los ficheros de vuelta xml y se requiere la intervención de usuario en la red de empuje para evitar que dos números de código estén presentes en la base de datos 32 que choca.

La Figura 11 ilustra una disposición alternativa, pero similar, a la Figura 10 – se asignan a características iguales signos de referencia iguales. El contenido del IN 18A de la red A se muestra después de que el IN 18A ha arrastrado datos relevantes desde dos VPN (la VPN X_B y la VPN Y_B) desde otra red (red B): la VPN X_B que tiene un acuerdo para permitir llamar en red entre VPN con la VPN X_A en la red A y la VPN Y_B que tiene un acuerdo para permitir llamar en red entre VPN con la VPN Y_A en la red A. Los números de código de la VPN X_B incluyen un identificador (que en este caso es el código de país "49" del país (Alemania) donde está alojada la VPN). Los dígitos del identificador preceden al número de código básico "60….67". De manera similar, los números de código de la VPN Y_B tienen un identificador "49" que precede el número de código básico relevante "1…8". Se tiene que señalar que las VPN se distinguen generalmente dentro del IN por identificadores separados que no se incluyen en los números de código. Estos identificadores de VPN separados son únicos dentro de esa red de alojamiento de VPN (aquí la red B), pero se podrían repetir en otra red.

Los números de código de la VPN X y la VPN Y, que están alojadas por la red A (y en la Figura 11 se designan VPN X_A y VPN Y_A) se pueden considerar que son VPN "locales". Ningún identificador (código de país) precederá tales números de código "locales" cuando se almacenan en el IN 18A. Cuando los datos de la VPN X_A e Y_A se cargan al sistema IMP 30, el adaptador 34A añadirá un identificador relevante (por ejemplo, un identificador equivalente al código de país) a fin de poner los datos de la VPN en el formato requerido para el sistema IMP 30.

Se debería entender que cualquier red puede alojar las VPN que solamente se requieren localmente dentro de esa red y donde los detalles de la cual nunca se pasan al sistema IMP 30.

Debido a que los números de código de las VPN locales (VPN X_A y VPN Y_A no se procesan por el adaptador 34A y el sistema IMP 30 y no se dotan con un identificador (código de país), es posible que un número de código usado por una VPN local sea el mismo que el número de código (prefijado) usado en los datos de VPN arrastrados. En la Figura 11, la tercera desde la última entrada de la columna de la izquierda para la VPN X_A tiene un número de código "4965". No obstante, uno de los números de código de la VPN X_B también es "4965", aunque este último número de código comprende el identificador (código de país) "49" y el número de código básico "65".

Tal situación se puede tratar de formas similares a la situación análoga, tratada en relación con la Figura 10.

El intercambio de datos que tiene lugar entre los elementos mostrados en la Figura 6 que ocurre durante la iniciación de una llamada desde el terminal móvil 1A que es miembro de la VPN X_A alojada por la red A al terminal móvil 20 que es miembro de la VPN M_B alojada por la red B y marcada por el terminal móvil 1A usando el código corto para el terminal móvil 20, se describirá ahora con referencia a la Figura 12.

El usuario del terminal móvil 1A será consciente de que el terminal móvil 20 no es un miembro de la misma VPN que el terminal móvil 1A. El usuario del terminal móvil 1A sabrá que la VPN de la que es miembro el terminal móvil 20 está alojada en Alemania y por lo tanto precederá el número de código por el código de país para Alemania “49”.

Un mensaje de iniciación de llamada 60, que incluirá el número de código marcado por el usuario del terminal móvil 1A, se transmite inalámbricamente desde el terminal móvil 1A al MSC 2A. El mensaje de iniciación entonces se transmite desde el MSC 2A al núcleo 12A (mensaje 61). El mensaje de iniciación incluye una marca u otro identificador que indica que la llamada se inicia para una VPN particular (la VPN M_B). Esta marca se identifica por el núcleo 12A. En la identificación de la marca, el núcleo 12A transmite el número de código extraído del mensaje de iniciación al IN 18A (mensaje 62). El IN 18A entonces consulta los datos almacenados dentro del mismo para localizar la entrada relevante para el número de código recibido. Por ejemplo, si el número de código del terminal móvil 20 es “12340”, el IN 18A entonces buscará inicialmente los datos almacenados para sus VPN locales (es decir, las VPN que aloja). Si, como en este caso, el número de código no se identifica como que es uno de una VPN local, la búsqueda se extiende entonces a los números de código de las VPN arrastradas previamente por el IN 18A desde el sistema IMP 30 usando el adaptador 34A. El IN 18A identificará el número de código 12340 almacenado para la VPN M_B y obtendrá el MSISDN relevante “+49 65 4521 2340”. El MSISDN se devuelve al núcleo 12A (mensaje 63) y este se transmite desde el núcleo 12A al MSC 2A (mensaje 64). El MSC 2A entonces modifica el mensaje de iniciación de llamada para incluir el MSISDN del terminal móvil llamado 20 en lugar del número de código. El mensaje de iniciación de llamada modificado entonces se transmite al núcleo 12A (mensaje 65), donde se maneja de una manera similar a cualquier otra llamada de teléfono iniciada usando un MSISDN convencional. No obstante, la marca que indica que la llamada es para un miembro de la VPN M_B se usa por el núcleo 12A para identificar y poner a disposición cualquier servicio especial que se ha acordado se proporcionará a las llamadas entre las VPN X_A y M_B y también para tarificar la llamada según la estructura de tarificación acordada entre esas VPN. El núcleo 12A identificará a partir de la estructura del MSISDN que la llamada es para un terminal móvil que es un abonado de la red B. El núcleo 12A de la red A entonces transmite el mensaje de iniciación de llamada al núcleo 12B de la red B a través de la interconexión 16 (mensaje 66). El mensaje entonces se encamina al MSC adecuado (MSC 6B) (mensaje 67) y de allí al terminal móvil 20 (mensaje 68). Cuando se acepta la llamada por el terminal móvil 20, la comunicación entre el terminal móvil 1A y el terminal móvil 20 puede ocurrir de la manera convencional.

Si un terminal móvil 1A en su lugar está transitando en la red B, el IN 34B de la red B permitirá el encaminamiento con éxito de las llamadas entre VPN y dentro de la VPN en virtud de los datos proporcionados a las mismas por el sistema IMP 30.

El uso de los códigos de país descritos anteriormente no es necesario si los números de código usados por todas las VPN son únicos y no hay duplicación de los números de código.

El IN de cada red se puede disponer de manera que, si el número de código de un miembro de una VPN alojada en esa red se marca por un abonado a esa red pero también incluyendo el prefijo usado para llamar a ese código desde otra red, la llamada aún se encaminará con éxito. Por ejemplo, si el código “4573” de un miembro de la VPN X_A (Figura 10) es prefijado con el código de país “44” para la red A por una persona que llama registrada con la red A, el IN 18A será capaz de encaminar la llamada al MSISDN 07771 225 4573 de la misma manera que si la persona que llama hubiera marcado simplemente el código corto “4573” sin el prefijo.

Como se mencionó anteriormente, una VPN simple puede abarcar una pluralidad de redes. Es decir, algunos miembros de una VPN se pueden registrar con la red A como su red doméstica y otros miembros de la VPN se pueden registrar con la red B como su red doméstica. Los códigos de los miembros de la VPN registrados con la red A tendrán el prefijo “44” añadido a los mismos (para marcar desde fuera de la red A, pero también se pueden marcar desde dentro de la red A con este prefijo) y de manera similar, los códigos de los miembros de la VPN registrados con la red B tendrán el prefijo “49” añadidos a los mismos (para marcar desde fuera de la red B, pero también se pueden marcar desde dentro de la red B con este prefijo).

En las realizaciones descritas anteriormente, los miembros de una VPN todos tienen un código (corto) que se puede usar para llamar a esa VPN. Las llamadas dentro de la VPN se pueden tarificar a tarifas de llamada especiales y/o se pueden proporcionar servicios especiales para tales llamadas. En una modificación, no se usan códigos cortos. En su lugar, los miembros de la VPN se llaman usando sus MSISDN. No obstante, la afiliación de la VPN se detecta por el IN de la red relevante, de manera que las tarifas de llamada especiales y/o servicios especiales se pueden proporcionar para tales llamadas (incluso aunque no se usen códigos cortos). La afiliación de la VPN de la parte llamada se puede detectar añadiendo una marca u otro identificador al miembro llamado que es interpretable por el núcleo de la red o por algún otro mecanismo. Por ejemplo, una tabla de búsqueda de los MSISDN que son miembros de la VPN se podría consultar cada vez que se recibe una llamada por el núcleo para determinar si la llamada es para un miembro de la VPN. La tabla de búsqueda se puede almacenar en el IN de cada red. El sistema

IMP 30 mantiene las tablas de búsqueda de una manera similar a aquella descrita anteriormente (donde se proporcionan códigos cortos) excepto, por supuesto, que los registros no necesitan incluir códigos cortos, sino solamente los MSISDN y datos de afiliación de la VPN.

Se debería apreciar que la invención también es aplicable a una disposición donde algunas o todas las redes A y B no son redes de telecomunicaciones celulares sino que son algún otro tipo de red de comunicaciones. Por ejemplo, una o más de las redes podrían ser una red de comunicaciones por satélite. Puede haber más de dos redes.

Las redes A, B están separadas y son discretas en el sentido de que tienen un núcleo separado para encaminar datos entre los dispositivos registrados con las mismas y/o en el sentido de que no comparten una red de acceso radio/transmisores-receptores de estación base. Las redes se pueden operar por diferentes entidades (legales) y/o tienen facilidades separadas para autenticar dispositivos de usuario y tarificar a los usuarios de dispositivos registrados con las mismas por el uso de la red.

REIVINDICACIONES

1. Un sistema de comunicaciones que incluye una pluralidad de redes de telecomunicaciones inalámbricas (A, B), cada una que incluye una red de acceso radio (3A, 3B, 4A, 5A, 5B, 7A, 7B, 8A, 8B, 9A, 9B) y una red central (como 12A), cada una de las cuales:

dota a los terminales de abonado (1A, 1B, 20) del mismo con un número de teléfono conocido públicamente respectivo para permitir que las comunicaciones sean dirigidas a cada terminal de abonado,

permite que los terminales de abonado (1A, 1B, 20) seleccionados del mismo sean asociados juntos en un grupo de manera que esos terminales de abonado (1A, 1B, 20) pueden dirigir las comunicaciones entre sí usando un código respectivo asignado a cada uno de los terminales de abonado (1A, 1B, 20) seleccionados e

incluye medios (18A, 18B) para traducir el código de cada uno de los terminales (1A, 1B, 20) seleccionados en el número de teléfono conocido públicamente correspondiente del mismo;

en donde el sistema además incluye medios (30) para mantener una base de datos (32) de los códigos y números de teléfono conocidos públicamente correspondientes de todas dichas redes (A, B) y para proporcionar a una de dichas redes (A, B) un número de teléfono conocido públicamente que corresponde a un código de un terminal de abonado (1A, 1B, 20) de otra de dichas redes (A, B) para permitir la comunicación desde un terminal de abonado (1A, 1B, 20) de dicha una de las redes para ser dirigida a un terminal de abonado (1A, 1B, 20) de dicha otra de las redes usando el código de este último terminal de abonado (1A, 1B, 20).

2. El sistema de la reivindicación 1, en donde cada red (A, B) se dota con medios de interfaz respectivos (34A, 34B) para intercambiar datos con los medios de mantenimiento de la base de datos (30).

3. El sistema de la reivindicación 2, en donde los medios de interfaz son operables para transmitir datos indicativos de sus códigos de red y números de teléfono conocidos públicamente correspondientes a los medios de mantenimiento de la base de datos (30).

4. El sistema de la reivindicación 3, en donde los medios de interfaz (34A, 34B) son operables para generar dichos datos en un formato predeterminado para uso por los medios de mantenimiento de la base de datos (30).

5. El sistema de la reivindicación 4, en donde los medios de interfaz (34A, 34B) son operables para generar dichos datos usando XML.

6. El sistema de una cualquiera de las reivindicaciones 2 a 5, en donde los medios de interfaz (34A, 34B) son operables para recibir datos indicativos de códigos y números de teléfono conocidos públicamente de otras de dichas redes (A, B) desde los medios de mantenimiento de la base de datos (30).

7. El sistema de la reivindicación 6, en donde dichos medios de mantenimiento de la base de datos (30) son operables para proporcionar solamente periódicamente los datos indicativos de dichos códigos y dichos números de teléfono conocidos públicamente correspondientes a los medios de traducción (18A, 18B).

8. El sistema de la reivindicación 6 o 7, en donde los medios de interfaz (34A, 34B) son operables para proporcionar los datos recibidos indicativos de dichos códigos y dichos números de teléfono conocidos públicamente correspondientes a los medios de traducción (18A, 18B) de manera que los medios de traducción (18A, 18B) son capaces de encaminar una comunicación identificada por uno de dichos códigos sin recibir datos adicionales desde los medios de mantenimiento de la base de datos (30).

9. El sistema de una cualquiera de las reivindicaciones 1 a 8, en donde los terminales de abonado (1A, 1B, 20) asociados con el grupo pertenecen a dos o más redes (A, B).

10. El sistema de una cualquiera de las reivindicaciones 1 a 9, que incluye medios para modificar dichos códigos para dotarlos con un indicador del grupo y/o la red con la que están asociados.

11. El sistema de una cualquiera de las reivindicaciones 1 a 10, que incluye medios (32) para detectar dos códigos idénticos.

12. El sistema de una cualquiera de las reivindicaciones 1 a 11, en donde dicho grupo comprende una red privada virtual, VPN.

13. El sistema de una cualquiera de las reivindicaciones 1 a 12, que incluye medios para identificar las comunicaciones iniciadas usando dicho código y para aplicar una tarificación especial o esquema de servicio a tales comunicaciones.

14. El sistema de una cualquiera de las reivindicaciones 1 a 13, que incluye medios para determinar si una llamada es una llamada en línea, que es una llamada entre terminales de abonado (1A, 1B, 20) en dos o más grupos entre los cuales existe un acuerdo para permitir que las llamadas sean encaminadas entre los mismos usando el código

respectivo asignado a cada uno de los terminales de abonado (1A, 1B, 20) o entre los cuales existe un acuerdo para unir los grupos en una asociación; y para aplicar un esquema de servicio especial a dicha llamada donde se determina que la llamada está en línea.

15. El sistema de la reivindicación 14, en donde la llamada se inicia por un terminal de abonado (1A, 1B, 20) que está asociado con un grupo dado de terminales de abonado y en donde los medios de determinación son operables para detectar si la comunicación fue iniciada usando un código asignado a un terminal de abonado asociado con dicho grupo dado, determinando por ello si la llamada está en línea.

16. El sistema de la reivindicación 14 o 15, en donde el grupo dado comprende una red privada virtual, VPN y cada terminal de abonado (1A, 1B, 20) que participa en dicha llamada pertenece a la misma VPN.

17. Un método de habilitación de comunicación entre una pluralidad de redes de telecomunicaciones inalámbricas, cada red (A, B) que incluye una red de acceso radio (3A, 3B, 4A, 4B, 5A, 5B, 7A, 7B, 8A, 8B, 9A, 9B) y una red central (12A), el método que incluye:

dotar a los terminales de abonado (1A, 1B, 20) de cada red con un número de teléfono conocido públicamente respectivo para permitir que las comunicaciones sean dirigidas a cada terminal de abonado (1A, 1B, 20)

asociar los terminales de abonado (1A, 1B, 20) seleccionados de cada red (A, B) juntos en un grupo de manera que esos terminales de abonado (1A, 1B, 20) pueden dirigir las comunicaciones entre sí usando un código respectivo asignado a cada uno de los terminales de abonado (1A, 1B, 20) seleccionados;

traducir el código de cada uno de los terminales (1A, 1B, 20) seleccionados al número de teléfono conocido públicamente correspondiente del mismo; y

mantener una base de datos (32) de los códigos y los números de teléfono conocidos públicamente correspondientes de todas dichas redes (A, B) y para proporcionar a una de dichas redes (A, B) un número de teléfono conocido públicamente que corresponde a un código de un terminal de abonado (1A, 1B, 20) de otra de dichas redes (A, B) para permitir la comunicación desde un terminal de abonado (1A, 1B, 20) de dicha una de las redes (A, B) para ser dirigida a un terminal de abonado (1A, 1B, 20) de dicha otra de las redes (A, B) usando el código de este último terminal de abonado (1A, 1B, 20).

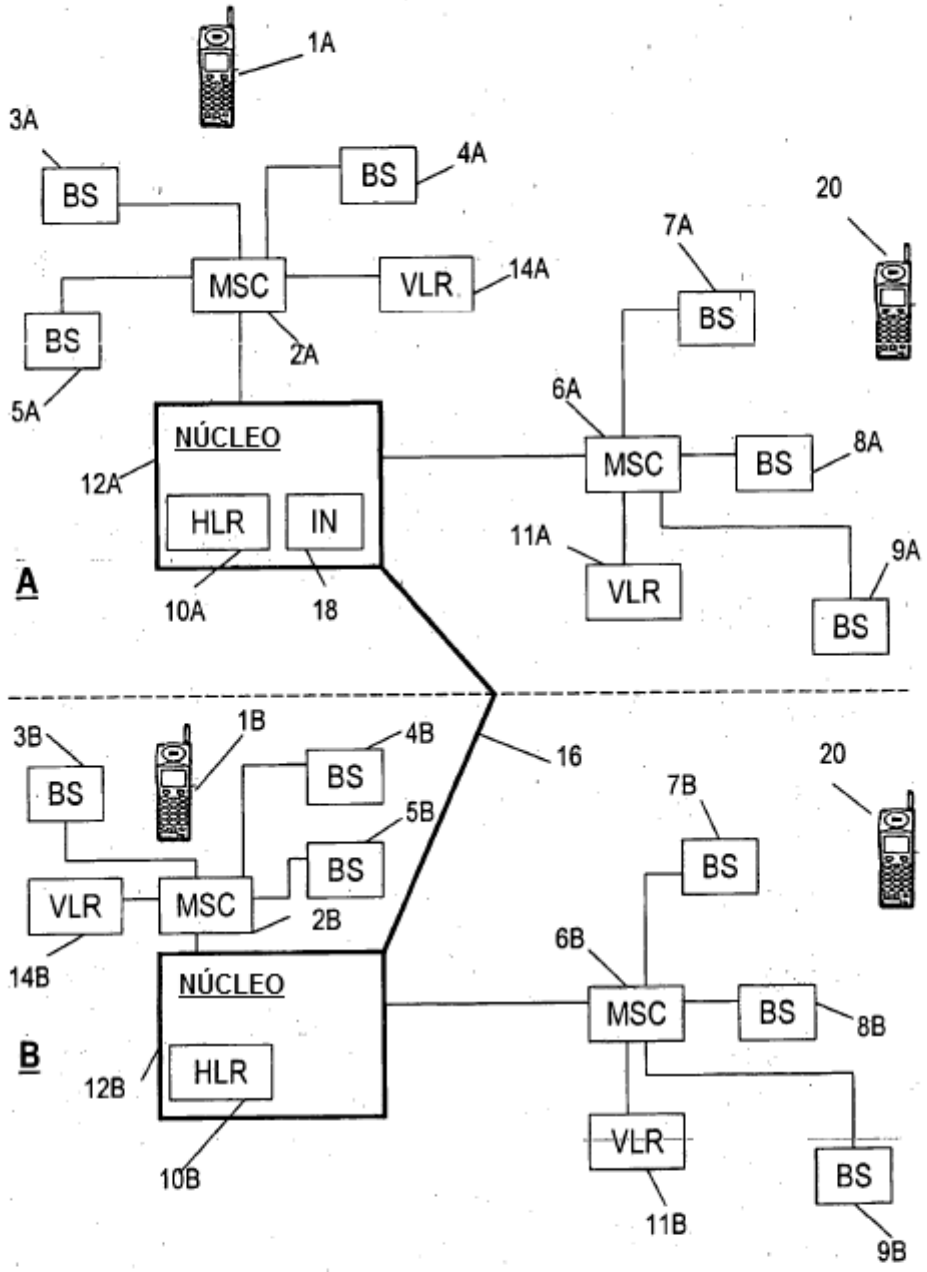

1A
3A
BS
BS
4A
MSC
VLR
14A
BS
2A
5A
NÚCLEO
12A
HLR
IN
10A
18
A
20
7A
BS
6A
MSC
BS
8A
11A
VLR
9A
BS
1B
3B
BS
4B
BS
16
5B
BS
VLR
MSC
2B
14B
NÚCLEO
B
12B
HLR
10B
20
7B
BS
6B
MSC
BS
8B
VLR
BS
11B
9B

FIG. 1

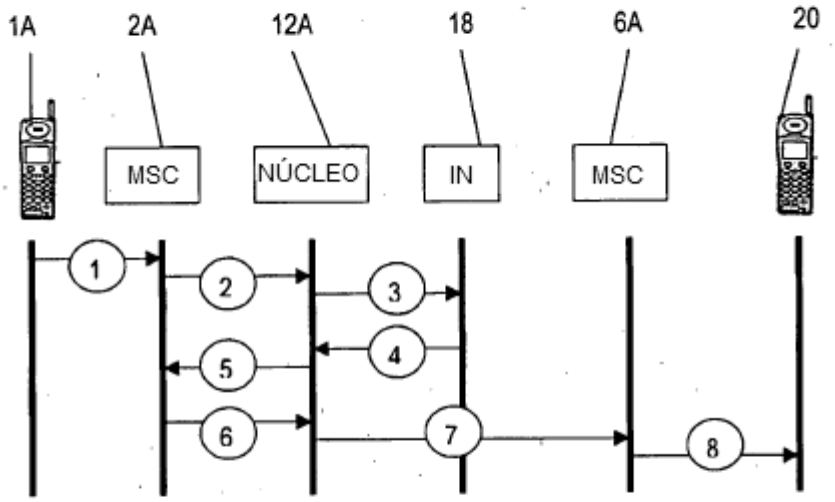


FIG. 2

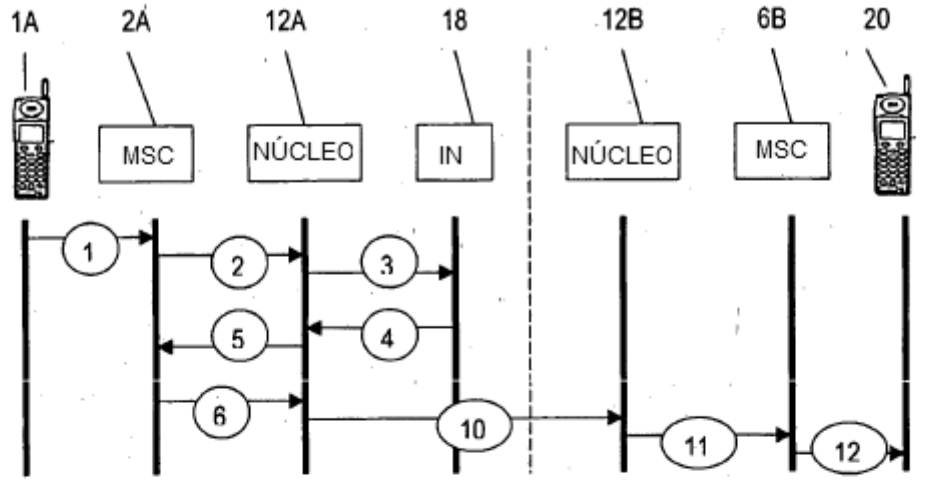

1A
2A
12A
18
12B
6B
20
MSC
NÚCLEO
IN
NÚCLEO
MSC
1
2
3
4
5
6
10
11
12

FIG. 3

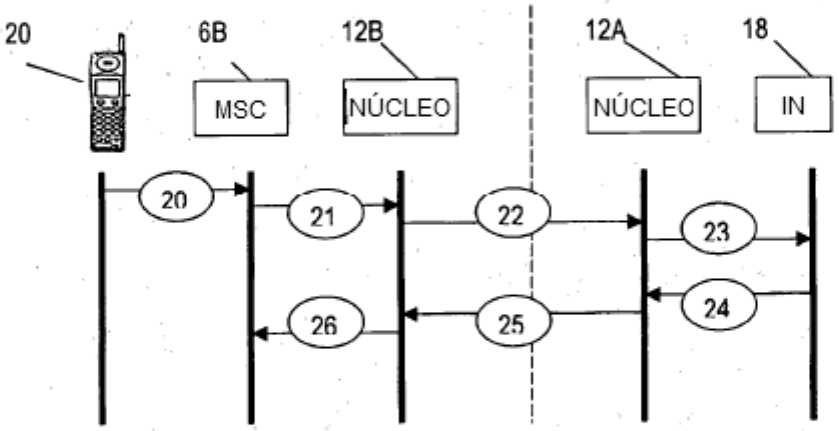

20
6B
12B
12A
18
MSC
NÚCLEO
NÚCLEO
IN
20
21
22
23
24
25
26

FIG. 4

IN 18			
VPN X		VPN Y	
Nº Código	MSISDN/Nº Teléfono	Nº Código	MSISDN/Nº Teléfono
0	0207 225 1000	100	07772 654 100
4573	07771 225 4573	101	07772 654 101
4574	07771 225 4574	102	07772 654 102
4575	07771 225 4575	103	07772 654 103
...	...	104	07772 654 104
4965	07771 225 4965	105	07772 654 105
4990	+49 89 2399 4990	106	07772 654 106
4491	+49 89 2399 4991	107	07772 654 107
...	...	...	...

FIG. 5

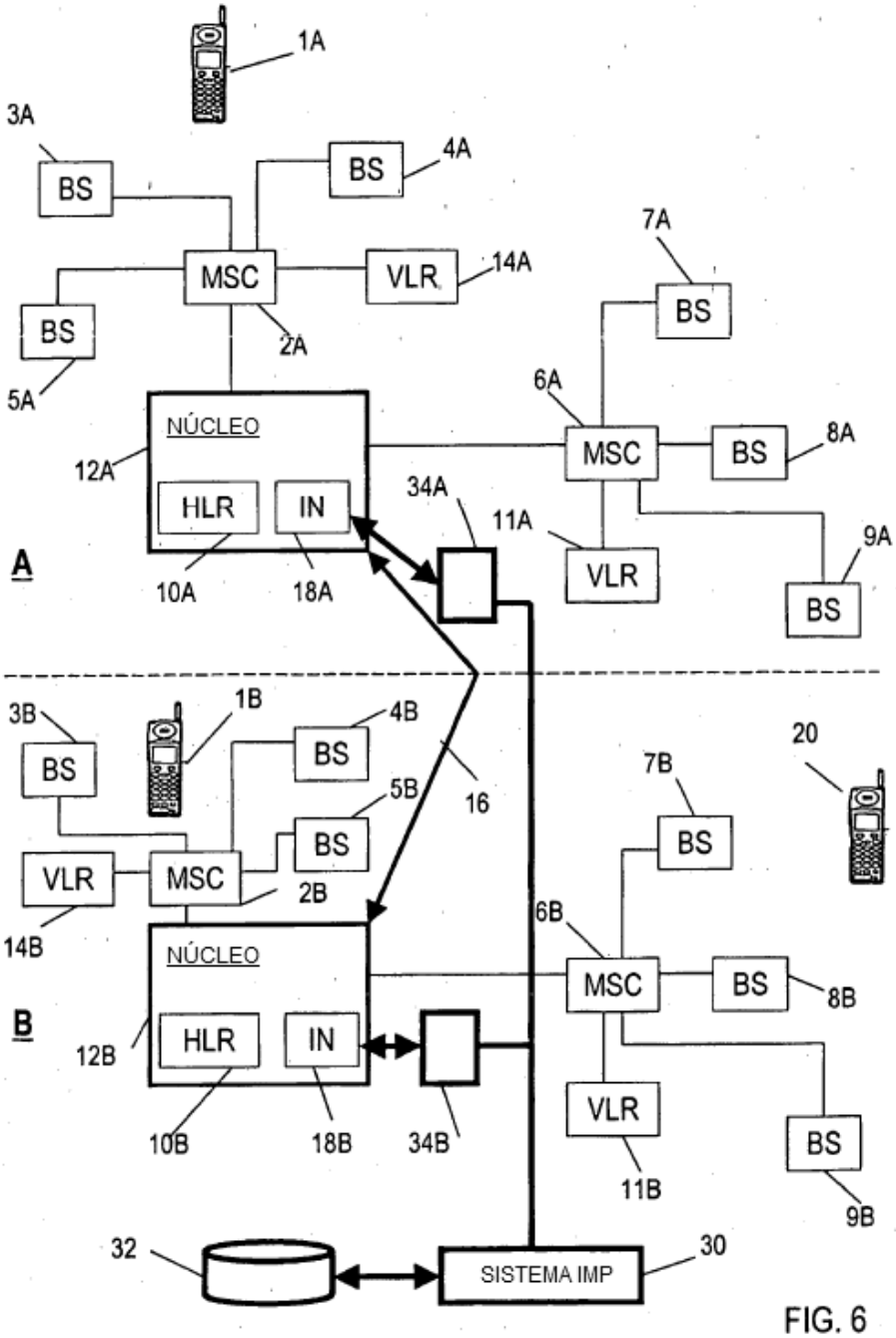

1A
3A
BS
4A
BS
MSC
VLR
14A
BS
2A
5A
7A
BS
6A
NÚCLEO
MSC
BS
8A
12A
HLR
IN
34A
11A
9A
A
10A
18A
VLR
BS
1B
3B
BS
4B
BS
20
7B
5B
16
BS
VLR
MSC
2B
6B
14B
NÚCLEO
MSC
BS
8B
B
12B
HLR
IN
VLR
BS
10B
18B
34B
11B
9B
32
SISTEMA IMP
30

FIG. 6

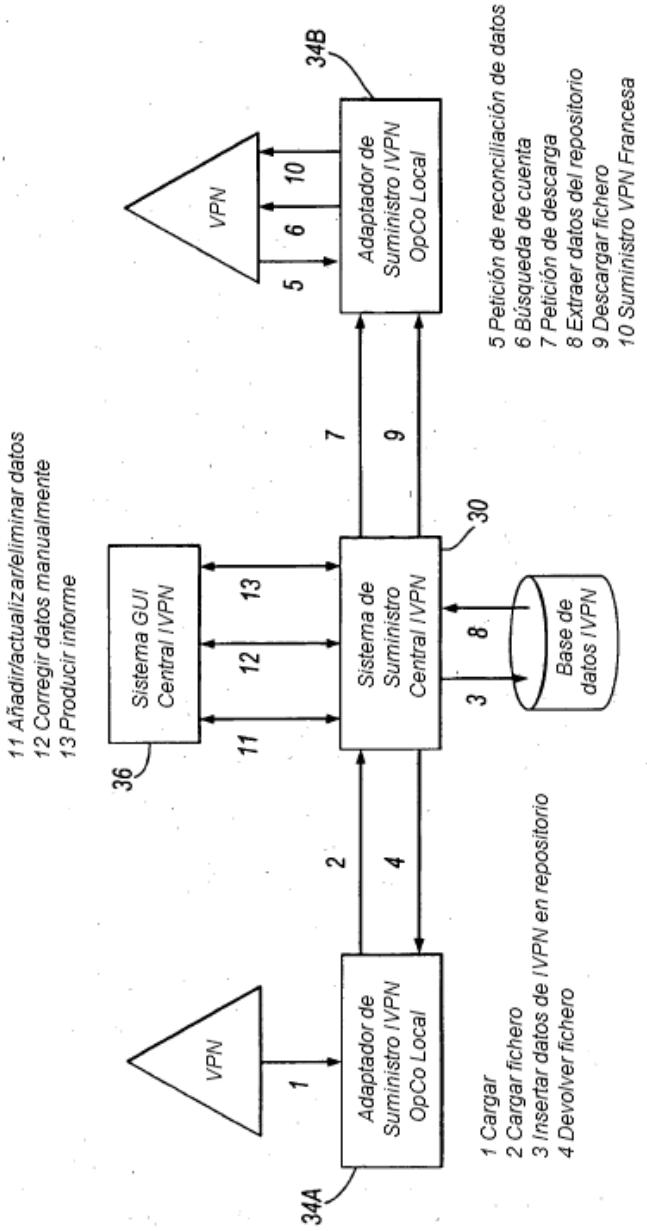

VPN
Adaptador de Suministro IVPN OpCo Local
34A
Sistema GUI Central IVPN
36
Sistema de Suministro Central IVPN
30
Base de datos IVPN
VPN
Adaptador de Suministro IVPN OpCo Local
34B
1 Cargar
2 Cargar fichero
3 Insertar datos de IVPN en repositorio
4 Devolver fichero
5 Petición de reconciliación de datos
6 Búsqueda de cuenta
7 Petición de descarga
8 Extraer datos del repositorio
9 Descargar fichero
10 Suministro VPN Francesa
11 Añadir/actualizar/eliminar datos
12 Corregir datos manualmente
13 Producir informe

Fig.7

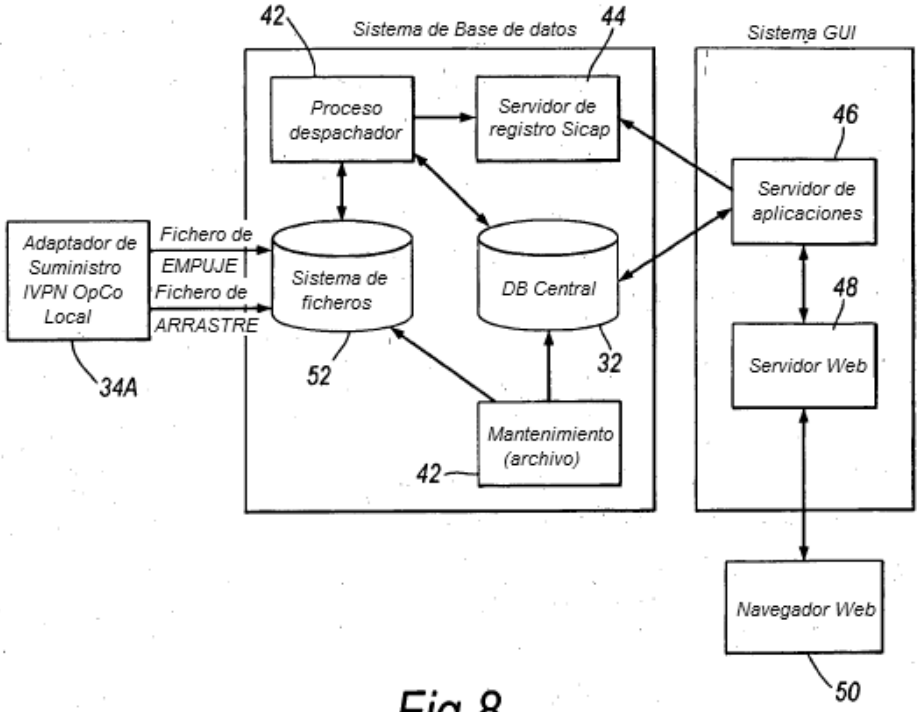
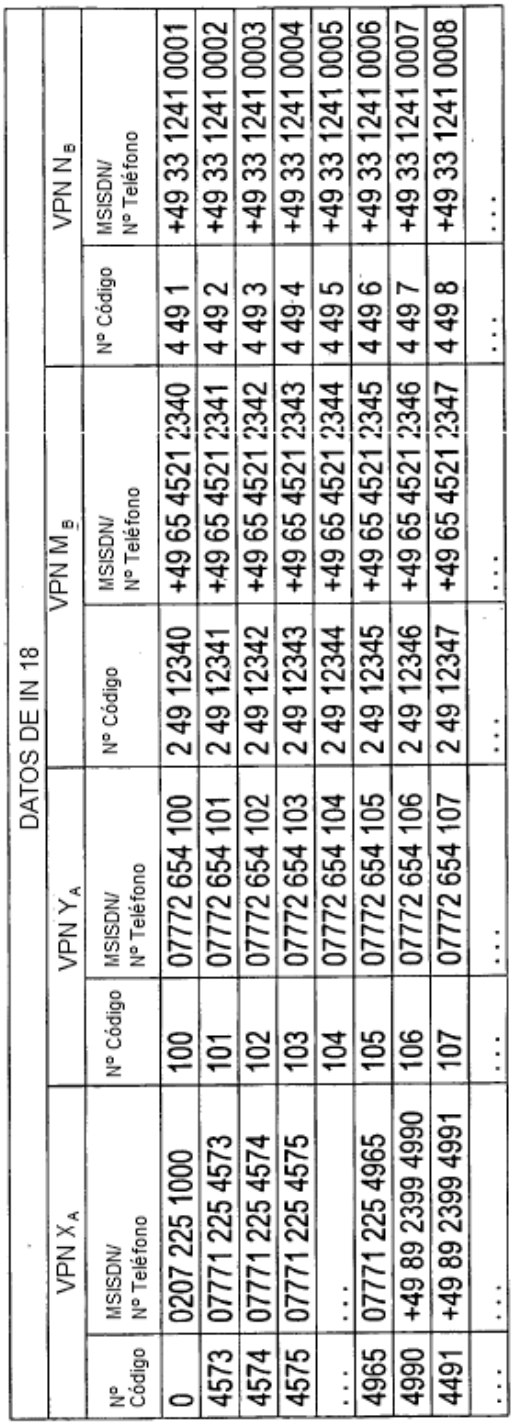

42
Sistema de Base de datos
44
Sistema GUI
Proceso despachador
Servidor de registro Sicap
46
Servidor de aplicaciones
Adaptador de Suministro IVPN OpCo Local
Fichero de EMPUJE
Fichero de ARRASTRE
Sistema de ficheros
DB Central
48
Servidor Web
34A
52
32
Mantenimiento (archivo)
42
Navegador Web
50

Fig.8

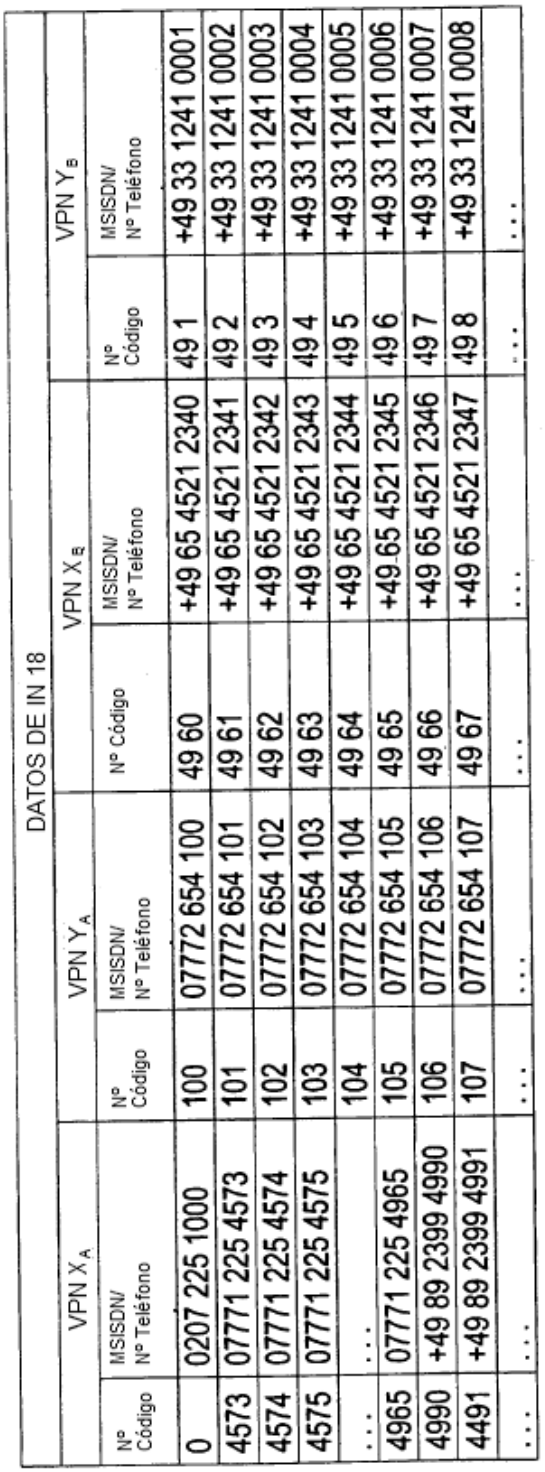
BASE DE DATOS DEL SISTEMA IMP 32							
VPN X_A		VPN Y_A		VPN M_B		VPN N_B	
Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono
1 44 0	+44 207 225 1000	5 44 100	+44 7772 654 100	2 49 12340	+49 65 4521 2340	4 49 1	+49 33 1241 0001
1 44 4573	+44 7771 225 4573	5 44 101	+44 7772 654 101	2 49 12341	+49 65 4521 2341	4 49 2	+49 33 1241 0002
1 44 4574	+44 7771 225 4574	5 44 102	+44 7772 654 102	2 49 12342	+49 65 4521 2342	4 49 3	+49 33 1241 0003
1 44 4575	+44 7771 225 4575	5 44 103	+44 7772 654 103	2 49 12343	+49 65 4521 2343	4 49 4	+49 33 1241 0004
...	...	5 44 104	+44 7772 654 104	2 49 12344	+49 65 4521 2344	4 49 5	+49 33 1241 0005
1 44 4965	+44 7771 225 4965	5 44 105	+44 7772 654 105	2 49 12345	+49 65 4521 2345	4 49 6	+49 33 1241 0006
1 44 4990	+49 89 2399 4990	5 44 106	+44 7772 654 106	2 49 12346	+49 65 4521 2346	4 49 7	+49 33 1241 0007
1 44 4491	+49 89 2399 4991	5 44 107	+44 7772 654 107	2 49 12347	+49 65 4521 2347	4 49 8	+49 33 1241 0008
...	...	...	...	...	...	...	...

FIG. 9



DATOS DE IN 18								
VPN X_A		VPN Y_A		VPN M_B		VPN N_B		
Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono
0	0207 225 1000	100	07772 654 100	2 49 12340	+49 65 4521 2340	4 49 1	+49 33 1241 0001
4573	07771 225 4573	101	07772 654 101	2 49 12341	+49 65 4521 2341	4 49 2	+49 33 1241 0002
4574	07771 225 4574	102	07772 654 102	2 49 12342	+49 65 4521 2342	4 49 3	+49 33 1241 0003
4575	07771 225 4575	103	07772 654 103	2 49 12343	+49 65 4521 2343	4 49 4	+49 33 1241 0004
...	...	104	07772 654 104	2 49 12344	+49 65 4521 2344	4 49 5	+49 33 1241 0005
4965	07771 225 4965	105	07772 654 105	2 49 12345	+49 65 4521 2345	4 49 6	+49 33 1241 0006
4990	+49 89 2399 4990	106	07772 654 106	2 49 12346	+49 65 4521 2346	4 49 7	+49 33 1241 0007
4491	+49 89 2399 4991	107	07772 654 107	2 49 12347	+49 65 4521 2347	4 49 8	+49 33 1241 0008
...	...	...	...	...	...	...	...

FIG. 10



DATOS DE IN 18

VPN X_A		VPN Y_A		VPN X_B		VPN Y_B	
Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono	Nº Código	MSISDN/ Nº Teléfono
0	0207 225 1000	100	07772 654 100	49 60	+49 65 4521 2340	49 1	+49 33 1241 0001
4573	07771 225 4573	101	07772 654 101	49 61	+49 65 4521 2341	49 2	+49 33 1241 0002
4574	07771 225 4574	102	07772 654 102	49 62	+49 65 4521 2342	49 3	+49 33 1241 0003
4575	07771 225 4575	103	07772 654 103	49 63	+49 65 4521 2343	49 4	+49 33 1241 0004
...	...	104	07772 654 104	49 64	+49 65 4521 2344	49 5	+49 33 1241 0005
4965	07771 225 4965	105	07772 654 105	49 65	+49 65 4521 2345	49 6	+49 33 1241 0006
4990	+49 89 2399 4990	106	07772 654 106	49 66	+49 65 4521 2346	49 7	+49 33 1241 0007
4491	+49 89 2399 4991	107	07772 654 107	49 67	+49 65 4521 2347	49 8	+49 33 1241 0008
...	...	...	...	...	...	...	...

FIG. 11

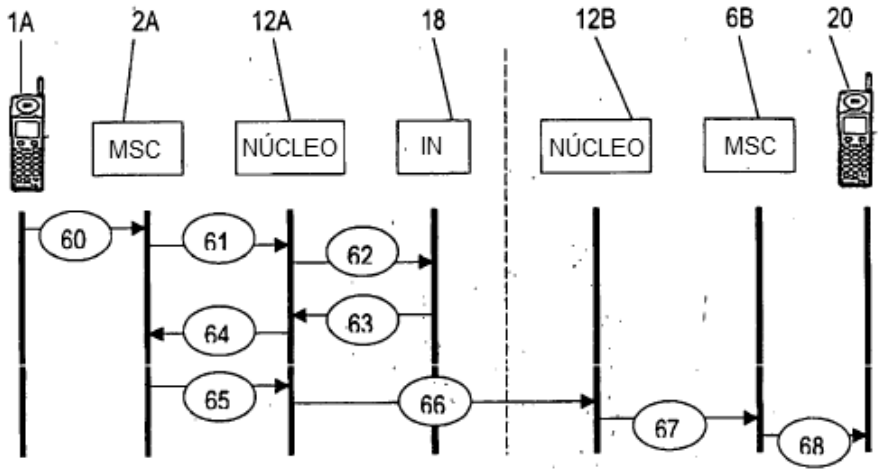

1A
2A
12A
18
12B
6B
20
MSC
NÚCLEO
IN
NÚCLEO
MSC
60
61
62
63
64
65
66
67
68

FIG. 12