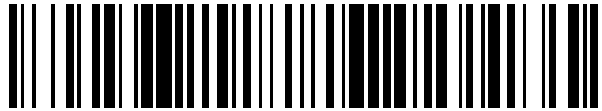


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 404 045**

51 Int. Cl.:

H04L 29/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **13.05.2008 E 08874305 (9)**

97 Fecha y número de publicación de la concesión europea: **27.02.2013 EP 2277298**

54 Título: **Manejo del tipo de usuario en una red de acceso inalámbrica**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
23.05.2013

73 Titular/es:

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

72 Inventor/es:

**VIKBERG, JARI y
NYLANDER, TOMAS**

74 Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

ES 2 404 045 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Manejo del tipo de usuario en una red de acceso inalámbrica

Campo técnico

5 La presente invención se refiere a las redes de telecomunicaciones inalámbricas. Más específicamente, y sin limitación, la invención se dirige a un método de informar a una Puerta de Enlace de Seguridad (SEGW – SEcurity GateWay, en inglés) y/o a un Controlador de Red de Acceso Genérica (GANC – Generic Access Network Controller, en inglés) acerca de diferentes tipos de usuario.

Antecedentes

10 El Proyecto de Colaboración de Tercera Generación (3GPP – Third Generation Partnership Project, en inglés) ha estandarizado el concepto de Red de Acceso Genérica (GAN – Generic Access Network, en inglés) a partir del 3GPP de Versión 6. El nombre más preciso utilizado por el 3GPP es “Acceso Genérico a Interfaces A/Gb” y esta estandarización estaba basada en las especificaciones de facto del Acceso mediante Telefonía Móvil Sin Licencia (UMA – Unlicensed Mobile Access, en inglés). Dos ejemplos de soluciones existentes para permitir que una Estación de Telefonía Móvil (MS – Mobile Station, en inglés) acceda a una Red de Núcleo (CN – Core Network, en inglés) de GSM son: una solución de GAN y una solución de tipo Femto para GSM.

15 La FIG. 1 es un diagrama de bloques funcional del TS 43.318 del 3GPP que ilustra una arquitectura de la GAN 10. La GAN se especifica en el TS 43.318 y el TS 44.318 del 3GPP. Una estación de telefonía Móvil (MS – Mobile Station, en inglés) 11 se conecta a través de un punto de acceso (AP – Access Point, en inglés) de WiFi en una red de acceso 12 de IP genérica. La GAN proporciona una nueva Red de Acceso por Radio (RAN – Radio Access Network, en inglés), y el nodo correspondiente al Controlador de Estación de Base de la GERAN se denomina Controlador de Red de Acceso Genérica (GANC – Generic Access Network Controller, en inglés) 13. El GANC 13 incluye una Puerta de Enlace de Seguridad (SEGW – SEcurity GateWay, en inglés) 14 y se conecta a una Red de Núcleo (CN – Core Network, en inglés) de GSM 15. La MS es un aparato de mano de modo dual, de radio dual, que incluye por ejemplo tanto WiFi como soporte de macro radio de 3GPP (por ejemplo, GSM, WCDMA o los dos). La MS se conecta al AP de WiFi utilizando la Radio de WiFi. El estándar de GAN define por ejemplo cómo puede funcionar la MS en modo de GAN y acceder a los servicios proporcionados por la CN de GSM utilizando la interfaz Up 16 entre la MS y el GANC.

La interfaz Up 16 puede atravesar redes de IP inseguras y está por lo tanto protegida mediante un túnel de IP seguro entre la MS 11 y el GANC 13 manejado por la SEGW 14.

30 La GAN estándar actual puede denominarse “GAN de 2G” (“2G-GAN” en inglés) o “GAN de GSM” (“GSM-GAN”, en inglés) porque las interfaz-A e interfaz-Gb de GSM estándar se utilizan entre el GANC y la CN. Se está trabajando para estandarizar una solución “GAN de 3G” (“3G-GAN”, en inglés) o “GAN de WCDMA” (“WCDMA-GAN”, en inglés). En este caso, el GANC utilizará interfaces de WCDMA estándar tales como las interfaces lu-cs e lu-ps para conectarse a la CN. El estándar resultante puede ser también denominado “Generic Access to lu Interfaces” o “lu de GAN” (“GAN-lu”, en inglés).

40 La FIG. 2 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de Circuitos Conmutados (CS – Circuit Switched, en inglés) 20 relacionada con la solución de la GAN y con la Interfaz Up 16. El GANC 13 utiliza señalización de interfaz A normal hacia el Centro de Conmutación de Telefonía Móvil (MSC – Mobile Switching Center, en inglés) 21. El GANC interrelaciona los protocolos relacionados, como la Parte de Aplicación del Sistema de Estación de Base (BSSAP – Base Station System Application Part, en inglés) 22, con los protocolos de GAN relevantes, tales como Recursos de Circuitos Conmutados para Acceso Genérico (GA-CSR – Generic Access-Circuit Switched Resources, en inglés) 23, en las dos direcciones.

45 La FIG. 3 es un diagrama de señalización que ilustra el procedimiento de registro de GAN existente entre la MS 11 y el GANC 13. Este procedimiento está bien definido, por ejemplo, en las Especificaciones Técnicas del 3GPP para GAN, por lo tanto el procedimiento no se describirá con detalle en esta memoria, aunque varias etapas son relevantes para la presente invención.

50 En la etapa 3, se establece un túnel de IPsec entre la MS y la SEGW 14 utilizando señalización de IKEv2. La MS soporta una tarjeta (U)SIM y el establecimiento del túnel es autenticado utilizando señalización de SIM de EAP o AKA de EAP entre la MS y el servidor de Autenticación, Autorización y Registro de Operaciones (AAA – Authentication, Authorization and Accounting, en inglés) 25 tal como requiere la SEGW. El procedimiento de autenticación es llevado a cabo realmente hacia la tarjeta (U)SIM en la MS. El AAA contacta a un HLR/AuC 26 para obtener las claves de seguridad requeridas para ser utilizadas como parte de la señalización de SIM de EAP o de AKA de EAP.

55 En la etapa 6, la MS 11 envía un mensaje de SOLICITUD DE REGISTRO DE RC de GA al GANC 13 y puede indicar alguna información acerca de las capacidades de la MS en el Elemento de Información (IE – Information Element, en inglés) de Marca de clase da la GAN.

En la etapa 7, el intento de registro de la GAN es aceptado por el GANC 13 y un mensaje de ACEPTAR REGISTRO DE RC de GA es devuelto a la MS 11. Los casos de rechazo y redireccionamiento tal como se muestran en las etapas 8 y 9 alternativas no son relevantes para la presente invención y se muestran sólo para completar.

5 La FIG. 4 es un diagrama de señalización que ilustra la secuencia de señalización de la GAN cuando se lleva a cabo una Actualización de Ubicación periódica en el modo de GAN. Las partes más relevantes de esta secuencia son las etapas 11-12 en las cuales el GANC 13 recibe una ORDEN DE MODO DE CODIFICACIÓN (BSSAP) y se supone que activará la señalización hacia la MS 11. Estas etapas particulares se utilizan en esta memoria como ejemplo de cómo debe actuar el GANC hacia los diferentes tipos de terminales y puntos de acceso que acceden al sistema.

10 La FIG. 5 es un diagrama de bloques funcional de una arquitectura de una red de acceso de tipo Femto para GSM. La solución de tipo Femto para GSM proporciona pequeñas femtoceldas para los usuarios finales teniendo pequeñas estaciones de base de radio de GSM, por ejemplo, en la casa del usuario. La estación de base de radio pequeña se denomina Equipo de la Casa del Abonado (CPE – Customer Premises Equipment, en inglés) de Femtoceldas 31. El CPE de Femtocelda se conecta a la red utilizando las interfaces Fp y Abis sobre IP propietarias. El nodo correspondiente al BSC de la GERAN se denomina BSC de tipo Femto 32. No existe ningún estado del 3GPP específico para la solución de tipo Femto para GSM. Una de las principales diferencias de la solución de GAN descrita anteriormente es que las MSs no requieren ningún cambio porque entre la MS y el CPE de Femtoceldas se utiliza la interfaz Um de GSM estándar. La MS se conecta al CPE de Femtoceldas como normalmente en la GERAN. El CPE de Femtoceldas es a continuación conectado al BSC de tipo Femto utilizando las interfaces Fp y Abis sobre IP propietaria.

20 La FIG. 6 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de CS 40 relativa a la solución de tipo Femto para GSM de la FIG. 6. El BSC de tipo Femto 32 utiliza señalización de interfaz A normal hacia el MSC 21. El BSC de tipo Femto interrelaciona los protocolos relacionados, como el BSSAP 22, con los protocolos de GSM relevantes tales como los recursos de Radio de GSM (GSM RR – GSM Radio Resources, en inglés) 41 en ambas direcciones.

25 La solución de seguridad aplicada a la solución de tipo Femto para GSM es muy similar a la solución utilizada en la GAN (como se ha descrito en la FIG. 3). El CPE de Femtocelda 31 establece un túnel de IPsec hacia la SEGW 14 utilizando los mismos mecanismos que en la GAN. La principal diferencia es que el CPE de la Femtocelda contiene la tarjeta (U)SIM que es autenticada hacia el servidor de AAA 25.

30 El documento US 2007/268888, 22 de Noviembre de 2007 (2007-11-22) describe un método que emplea comunicaciones entre un controlador de red de acceso, una puerta de enlace de seguridad (SGW – Security GateWay, en inglés) y un servidor de AAA para mejorar la funcionalidad de la red. La SGW se comunica con el servidor de AAA para facilitar la autenticación de una estación de telefonía Móvil. La autenticación puede implicar determinar qué características de la red y/o servicios está la estación de telefonía Móvil autorizada a utilizar y/o es capaz de utilizar. La IMSI de la estación de telefonía Móvil puede ser comparada con los criterios de IMSI predeterminados por el servidor de AAA para determinar si autorizar o no a la estación de telefonía Móvil para ciertas comunicaciones a través de la red. La información de seguridad compartida entre la SGW, el servidor de AAA y el controlador de la red incluye la IMSI de la estación de telefonía Móvil, capacidades de abonado, perfiles de QoS y otra información de la red que permite que la SGW tome decisiones inteligentes sobre cómo tratar una sesión de usuario dada.

40 **Compendio**

En diferentes realizaciones, la presente invención proporciona información del tipo de usuario a la SEGW o permite que la SEGW obtenga información del tipo de usuario para diferentes tipos de usuario de manera que la SEGW pueda aplicar funciones de seguridad específicas basándose en el tipo de usuario. La invención es aplicable a todas las soluciones en las que se utiliza un componente tal como la SEGW. La invención puede proporcionar también información del tipo de usuario a un nodo de control tal como un GANC o permitir que el GANC obtenga información del tipo de usuario para la aplicación de ajustes de seguridad hacia los clientes de la GAN.

50 En una realización, la presente invención se dirige a un método en una red de acceso inalámbrica para proporcionar una indicación del tipo de usuario a una Puerta de Enlace de Seguridad (SEGW – SEcurity GateWay, en inglés) durante un procedimiento de registro para un usuario. El método incluye las etapas de recibir en un servidor de Autenticación, Autorización y Registro de Operaciones (AAA – Authentication, Authorization and Accounting, en inglés), una solicitud de autenticar al usuario; y enviar una indicación del tipo de usuario para el usuario desde el servidor de AAA a la SEGW con un mensaje de éxito de autenticación. La indicación del tipo de usuario puede crearse en el servidor de AAA o puede ser obtenida por el servidor de AAA a partir del Registro de Ubicación Local (HLR – Home Location Register, en inglés).

55 En otra realización, la presente invención se dirige a un método en una red de acceso inalámbrica para determinar información del tipo de usuario en una SEGW durante un procedimiento de registro para un usuario. El método incluye las etapas de configurar la SEGW con la información del tipo de usuario asociada con diferentes Identidades de Estación de Telefonía Móvil Internacional (IMSI – International Mobile Station Identities, en inglés) o números de

serie de IMSI; recibir la IMSI del usuario en la SEGW durante el procedimiento de registro; y determinar la información del tipo de usuario para el usuario basándose en la IMSI del usuario o en un número de serie de IMSI asociado.

5 En cualquiera de las dos realizaciones anteriores, el procedimiento de registro puede ser llevado a cabo en una Red de Acceso Genérica (GAN – Generic Access Network, en inglés), y la SEGW puede también enviar la información del tipo de usuario a un Controlador de Red de Acceso Genérica (GANC – Generic Access Network Controller, en inglés).

10 En otra realización, la presente invención se dirige a un método en una red de acceso inalámbrica para obtener información del tipo de usuario por parte de un nodo controlador durante un procedimiento de registro para un usuario. El método incluye las etapas de configurar una base de datos con información del tipo de usuario asociada con diferentes IMSIs o números de serie de IMSI; recibir la IMSI del usuario en el nodo controlador durante el procedimiento de registro; y utilizar la IMSI del usuario por parte del nodo controlador para obtener la información del tipo de usuario para el usuario a partir de la base de datos.

15 En otra realización, el propio nodo controlador está configurado con la información del tipo de usuario asociada con diferentes IMSIs o números de serie de IMSI. Cuando el nodo controlador recibe la IMSI del usuario durante el procedimiento de registro, el nodo controlador utiliza la IMSI del usuario para determinar la información del tipo de usuario para el usuario.

20 En otra realización, la presente invención se dirige a un servidor de AAA para proporcionar una indicación del tipo de usuario a una SEGW durante un procedimiento de registro para un usuario. El servidor de AAA incluye un medio para recibir una solicitud de autenticar al usuario; y un medio para enviar una indicación del tipo de usuario para el usuario a la SEGW con un mensaje de éxito de autenticación. El servidor de AAA puede crear la información del tipo de usuario internamente, o puede obtener la indicación del tipo de usuario de un HLR.

25 En otra realización, la presente invención se dirige a un aparato en una SEGW en una red de acceso. El aparato incluye una base de datos configurada para asociar información del tipo de usuario con diferentes IMSIs o números de serie de IMSI; un medio para recibir una IMSI de usuario durante un procedimiento de registro; y un medio para determinar información del tipo de usuario para el usuario basándose en la IMSI del usuario o en un número de serie de IMSI asociado.

30 En otra realización, la presente invención se dirige a un sistema en una red de acceso para proporcionar información del tipo de usuario a un nodo controlador durante un procedimiento de registro para un usuario. El sistema incluye una base de datos configurada para asociar información del tipo de usuario con diferentes IMSIs o números de serie de IMSI; un medio dentro del nodo controlador para recibir la IMSI del usuario durante un procedimiento de registro; y un medio dentro del nodo controlador para utilizar la IMSI del usuario con el fin de obtener información del tipo de usuario para el usuario de la base de datos.

35 Alternativamente, el nodo controlador puede ser configurado internamente con información del tipo de usuario asociada con diferentes IMSIs o números de serie de IMSI. Cuando el nodo controlador recibe la IMSI del usuario durante el procedimiento de registro, el nodo controlador utiliza la IMSI del usuario para determinar la información del tipo de usuario para el usuario.

Breve descripción de los dibujos

40 En lo que sigue, las características esenciales de la invención se describirán con detalle mostrando realizaciones preferidas, con referencia a las figuras adjuntas, en las cuales:

la FIG.1 es un diagrama de bloques funcional del TS 43.318 del 3GPP que ilustra una arquitectura de la Red de Acceso Genérica (GAN – Generic Access Network, en inglés);

la FIG. 2 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de circuitos conmutados (CS – Circuit Switched, en inglés) relativa a la solución de GAN de la FIG. 1;

45 la FIG. 3 es un diagrama de señalización que ilustra el procedimiento de registro de GAN existente entre una MS y un GANC;

la FIG. 4 es un diagrama de señalización que ilustra la secuencia de señalización de GAN existente cuando se lleva a cabo una Actualización de Ubicación periódica en el modo de GAN;

la FIG. 5 es un diagrama de bloques funcional de una arquitectura de una red de acceso de tipo Femto para GSM;

50 la FIG. 6 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de CS relativa a la solución de tipo Femto para GSM de la FIG. 5;

la FIG. 7 es un diagrama de bloques funcional de una arquitectura de una red de acceso de tipo Femto para GSM de GAN adecuada para su uso en la implementación de la presente invención;

la FIG. 8 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de CS relativa a la red de acceso de tipo Femto para GSM de GAN de la FIG. 7;

la FIG. 9 es un diagrama de bloques funcional de una arquitectura de una red de acceso de tipo Femto de WCDMA de GAN adecuada para su uso en la implementación de la presente invención;

5 la FIG. 10 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de CS relativa a la red de acceso de tipo Femto de WCDMA de GAN de la FIG. 9;

la FIG. 11 es un diagrama de señalización que ilustra dos tipos diferentes de Registros de GAN llevados a cabo por el CPE de Femtocelda hacia el GANC;

10 la FIG. 12 es un diagrama de señalización que ilustra un método existente de llevar a cabo señalización de IKEv2 y autenticación de SIM/AKA de EAP;

la FIG. 13 es un diagrama de señalización que ilustra una extensión de la FIG. 12 para implementar una configuración basada en HLR para informar a la SEGW de diferentes tipos de Usuario;

la FIG. 14 es un diagrama de señalización que ilustra una extensión de la FIG. 12 para implementar una configuración basada en AAA para informar a la SEGW de diferentes tipos de Usuario; y

15 la FIG. 15 es un diagrama de señalización que ilustra una realización de la presente invención para proporcionar información del tipo de usuario al GANC.

Descripción detallada

20 La FIG. 7 es un diagrama de bloques funcional de una arquitectura de una red de acceso de tipo Femto para GSM de GAN 50 adecuada para su uso en la implementación de la presente invención. Para desarrollar una solución de acceso con ventajas sobre la solución de GAN o la solución de tipo Femto para GSM, se puede combinar las dos soluciones, utilizando las mejores propiedades de cada una. La solución combinada permite la utilización de MSs existentes porque se usa la interfaz Um entre la MS 11 y un CPE de Femtocelda 51 modificado. El CPE de Femtocelda en una solución combinada es modificado para incluir un cliente de GAN, permitiendo que la interfaz Up sea utilizada para conectar el CPE de Femtocelda 51 al GANC 13. La interfaz Up estandarizada requiere algunas modificaciones, y así, se utiliza una llamada interfaz Up+. El GANC utiliza las interfaces de GSM normales hacia la CN 15 y los otros nodos de soporte como en la solución de GAN normal.

30 La FIG. 8 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de CS 60 relativa a la red de acceso de tipo Femto para GSM de GAN combinada de la FIG. 7. El CPE de Femtoceldas 51 se extiende con la funcionalidad de BSC 61 y con un cliente de GAN 62. La funcionalidad de BSC es necesaria para terminar el protocolo de RR de GSM desde la MS 11 y el cliente de GAN es necesario para interactuar entre el protocolo de RR de GSM y de CSR de GA. El GANC 13 interactúa entonces entre los protocolos de CSR de GA y el BSSAP.

35 La solución de seguridad aplicada para la red de tipo Femto de GSM de GAN 50 es muy similar a la solución utilizada en la solución de tipo Femto para GAN y para GSM. El CPE de Femtoceldas 51 establece un túnel de IPsec a la SEGW 14 utilizando los mismos mecanismos que en la GAN. La principal diferencia hacia la GAN es que el CPE de Femtocelda contiene la tarjeta (U)SIM que es autenticada hacia un servidor de AAA 25 (y esto es exactamente lo mismo que en la solución de tipo Femto para GSM).

40 La FIG. 9 es un diagrama de bloques funcional de una arquitectura de una red de acceso de tipo Femto de WCDMA de GAN 70 adecuada para su uso en la implementación de la presente invención. En este caso, la interfaz lu normal es utilizada entre el GANC y el lado de la red de núcleo de telefonía móvil y la interfaz aérea hacia las MSs es la interfaz Uu. Un CPE de Femtoceldas 71 modificado es modificado para incluir una funcionalidad de Controlador de Red de Radio (RNC – Radio Network Controller, en inglés) de UTRAN.

45 La FIG. 10 es un diagrama de protocolo que ilustra una Arquitectura de Plano de Control del Dominio de CS 80 relativa a la red de acceso de tipo Femto de WCDMA de la FIG. 9. Como se ha observado, el CPE de Femtoceldas 71 está modificado para incluir la funcionalidad de RNC de UTRAN en las capas de Control del Recurso de Radio (RRC – Radio Resource Control, en inglés) 81, de Control del Enlace de Radio (RLC – Radio Link Control, en inglés) 82 y de Control de Acceso a Medios (MAC – Media Access Control, en inglés) 83.

50 La FIG. 11 es un diagrama de señalización que ilustra dos tipos diferentes de Registros de GAN llevados a cabo por el CPE de Femtoceldas 51 hacia el GANC 13. Los dos tipos de registros se denominan Registro de GAN de CPE y Registro de GAN de MS. El Registro de GAN de CPE se lleva a cabo cuando el CPE de Femtoceldas 51 es encendido y se crea la femtocelda asociada. Después de que el CPE de Femtoceldas 51 envía un mensaje de SOLICITAR REGISTRO DE RC DE GA al GANC 13, el GANC devuelve un mensaje de ACEPTAR REGISTRO DE RC DE GA con la información del sistema de la GAN necesaria para el establecimiento de la femtocelda por el CPE de Femtoceldas.

- 5 El Registro de la GAN de la MS es llevado a cabo por el CPE de Femtoceldas 51 cuando detecta que una MS 11 está tratando de acceder a la femtocelda. Esto sucede normalmente cuando la MS lleva a cabo un procedimiento de Actualización de Ubicación a través de la femtocelda porque la femtocelda tiene un Identificador de Área de Ubicación (LAI – Location Area Identifier, en inglés) diferente comparado con las macro celdas del área. Después de que el CPE de Femtoceldas 51 envía un mensaje de SOLICITAR REGISTRO DE RC DE GA al GANC 13, el GANC devuelve un mensaje de ACEPTAR REGISTRO DE RC DE GA con información del sistema de la GAN. Después de esto, la MS puede acceder a servicios proporcionados por el GANC, es decir, la MS tiene acceso tanto al MSC como al SGSN.
- 10 El GANC 13 es capaz de combinar estos dos procedimientos. En otras palabras, el GANC es capaz de averiguar que el REGISTRO DE GAN DE MS se refiere a un REGISTRO DE GAN DE CPE (puesto que se utiliza el mismo túnel de IPsec).
- La presente invención se refiere al uso de nodos comunes en las diferentes realizaciones descritas anteriormente. Los nodos comunes y los principios relacionados como sigue:
1. SEGW (Puerta de Enlace de Seguridad – SEcurity GateWay, en inglés)
- 15 Todas las realizaciones descritas en esta memoria utilizan túneles de IPsec para acceder a la red. Estos túneles de IPsec están establecidos entre la MS 11 y la SEGW 14 (en la GAN) o entre el Punto de Acceso Local (HAP – Home Access Point, en inglés), por ejemplo el CPE de Femtoceldas y la SEGW. Esto significa que la SEGW es un nodo común entre estas realizaciones. Las diferentes realizaciones, no obstante, tienen diferentes tipos de requisitos de seguridad que la SEGW debe hacer cumplir sobre los túneles de IPsec. Estos requisitos se refieren por ejemplo al número de conexiones de TCP/flujo de UDP en el túnel o al ancho de banda total permitido en el túnel. Una razón clara para las diferencias es que en la GAN, existe un solo túnel de IPsec para cada MS, y en las otras soluciones, todas las MSs que acceden a un HAP comparten el mismo túnel de IPsec.
- 20 2. GANC (Controlador de GAN – GAN Controller, en inglés) u otro Nodo Controlador.
- 25 Hay un trabajo de estandarización en curso para soluciones distintas de la GAN que utilizan la SEGW 14, y todas las soluciones incluyen alguna forma de puerta de enlace o nodo controlador para controlar el registro de la MS. Aunque la presente invención se describe en esta memoria en términos de la GAN, debe entenderse que la invención es aplicable a cualquier tipo de puerta de enlace o nodo controlador que controle el registro de la MS y se comunique con la SEGW.
- 30 La GAN, la red de tipo Femto para GSM de GAN, y la red de tipo Femto para WCDMA de GAN contienen todas ellas el GANC 13. Existen, no obstante, algunas diferencias funcionales en cómo funciona el GANC por ejemplo hacia la MS habilitada con GAN y un HAP que utiliza la GAN. El GANC puede aplicar algunos ajustes de seguridad hacia los clientes de la GAN.
- 35 Otra diferencia de ejemplo se refiere al procedimiento de Control del Modo de Codificación como se describe en el TS 48.008 del 3GPP y se utiliza en el contexto de la “A/Gb de la GAN”. El procedimiento de control del modo de codificación permite que el MSC 21 pase información del modo de codificación al GANC 13 para seleccionar y cargar los datos del usuario y señalar al dispositivo de codificación con la clave apropiada.
- 40 No obstante, en el modo de GAN, toda la comunicación entre la MS 11 y la SEGW 14 es codificada utilizando el túnel de IPsec y no hay ninguna necesidad de claves de codificación. Esto significa que cuando el GANC recibe el mensaje de ORDEN DE MODO DE CODIFICACIÓN, sólo envía el algoritmo para ser utilizado en un “índice de clave” a la MS, la cual almacena la información para un posible uso futuro tras una transferencia a la GERAN. El mensaje de ORDEN DE MODO DE CODIFICACIÓN también incluye la clave de codificación, llamada Kc, que es normalmente utilizada por el BSC y la BTS para modificar la interfaz aérea hacia la MS. Como se ha descrito anteriormente, no obstante, el GANC no transmite la clave Kc.
- 45 Hay una necesidad diferente en la red de tipo Femto para GSM de GAN para el manejo del procedimiento de Control de Modo de Codificación. En este caso, el túnel de IPsec sólo se utiliza para codificar el tráfico entre el GANC 13 y el HAP 71. La interfaz aérea entre la MS 11 y el HAP es una interfaz aérea de GSM estándar y esto significa que la información de “Kc” es necesaria en el HAP para poder codificar/descodificar esta interfaz aérea hacia la MS.
- Así, el GANC 13 necesita saber si el Registro de la GAN y todos los procedimientos relativos al tráfico se refieren a una MS de GAN o a una MS que accede a través del HAP 71.
- 50 No se conoce ninguna solución para informar a la SEGW 14 de modo común acerca de los diferentes tipos de usuario.
- Una posible solución para informar al GANC 13 de nodo común de los tipos de usuario es extender la información de marca de Clase de la GAN que se incluye en el mensaje SOLICITAR REGISTRO DE RC DE GA para indicar “HAP” o “MS tras el HAP”. El GANC puede entonces utilizar esta información para actuar de manera diferente hacia la MS de la GAN o la “MS tras el HAP” (y también hacia el “HAP”). Este planteamiento, no obstante, tiene varios
- 55

problemas. Primero, el planteamiento depende de la MS (o del cliente de la GAN) que accede al sistema para establecer esta información correctamente. Esto no es aceptable porque un cliente de GAN falso podría establecer estos ajustes para reducir las restricciones de seguridad aplicadas y para recibir información sensible (como la “Kc” de la red). En segundo lugar, este planteamiento no proporciona la indicación del tipo de usuario a la SEGW 14.

- 5 Para resolver el segundo problema, puede implementarse un protocolo entre el GANC 13 y la SEGW 14 de manera que el GANC pueda informar a la SEGW acerca del tipo de usuario basándose en la información que el GANC recibió del cliente. No obstante, esto sería también un riesgo de seguridad en el caso de un cliente malicioso. Además, tal planteamiento significaría que el cliente ha accedido ya a la red sin que la SEGW conozca el tipo de usuario. Puesto que la SEGW es el punto de entrada a la red de telefonía móvil y el primer punto de contacto en el
10 que se verifica la identidad del usuario, deben aplicarse ajustes de seguridad desde la SEGW.

En la presente invención, la red está configurada con información acerca de una asociación entre la (U)SIM y el tipo de usuario. Por esta razón, la red no tiene que confiar en que el cliente indique un tipo de usuario específico. La invención permite que la SEGW 14 obtenga información acerca de diferentes tipos de usuario y aplique funciones de seguridad basándose en el tipo de usuario. Así, la invención es aplicable a todas las soluciones en las que se utilice un componente tal como la SEGW 14. Por ejemplo, los conceptos de la invención descritos en esta memoria son
15 aplicables, al menos para las siguientes soluciones:

- WLAN de Interacción (I-WLAN – Interworking WLAN, en inglés);

en este caso la SEGW es una Puerta de Enlace de Datos en Paquetes (PDG – Packet Data Gateway, en inglés).

- Acceso de IP distinto de 3GPP no fiable en el SAE/LTE;

20 en este caso la SEGW es la Puerta de Enlace de Datos en Paquetes evolucionada (ePDG – Evolved Packet Data Gateway, en inglés).

- de tipo Femto para GSM, de tipo Femto para WCDMA y de tipo Femto para LTE;
- UMA/GAN; y
- Combinación de UMA/GAN y solución de tipo Femto para GSM/WCDMA.

25 Se usan diferentes realizaciones de la presente invención para ilustrar cómo obtiene la SEGW 14 información de tipo de usuario, y cómo el GANC 13 conoce esta información. La SEGW puede ser informada utilizando una configuración basada en HLR, una configuración basada en AAA o una configuración basada en SEGW. El GANC puede ser informado por la SEGW después de que la SEGW obtiene la información a través de una de las configuraciones denotadas. Alternativamente, el GANC puede ser informado utilizando una configuración basada en
30 GANC o una configuración basada en la base de datos de la GAN. Debe observarse también que las realizaciones anteriores pueden ser combinadas de diferentes maneras.

La FIG. 12 es un diagrama de señalización que ilustra un método existente de llevar a cabo señalización de IKEv2 y autenticación de SIM/AKA de EAP en la solución de GAN. El procedimiento de autenticación de la FIG. 12 es
35 reproducido en la Figura A.1 de la especificación técnica TS 43.318 v8.0.0 del 3GPP, y no se explicará con más detalle excepto en el contexto de modificaciones y extensiones asociadas con las diferentes realizaciones de la presente invención que se describen a continuación.

La descripción que sigue presume que los diferentes “tipos de Usuario” están coordinados entre los diferentes nodos. Por ejemplo, la SEGW 14 y el GANC 13 conocen los diferentes tipos de usuario y tienen una lógica predefinida que depende del tipo de usuario. Los tipos de usuario pueden incluir, por ejemplo, “Punto de Acceso
40 Local”, “HAP de GSM”, “HAP de WCDMA”, “HAP de LTE”, y otros similares.

Tabla 1

Tipo de Usuario	Ancho de Banda Permitido (kbit/s)	Nº de TCP	Nº de UDP	Puertos de Destino Permitidos	IP/subred de Destino Permitida	Protocolos Permitidos	Nº de IPsec SA Permitido	Paquetes por segundo permitidos
Por defecto	100	2	2	14001-14010 24000-24500 53	192.160.0.0/16 192.159.1.50	TCP, UDP	2	20
HAP de GSM	200	4	4	12000-12400	192.168.0.0/16	TCP, UDP	4	100
WCDMA a HAP	1000	6	6	12500-13000	192.169.0.0/16	TCP/UDP, SCTP	8	500

La Tabla 1 anterior proporciona un ejemplo de cómo puede ser configurada la SEGW 14 para los diferentes “tipos de usuario”. Estos ejemplos definen limitaciones para cada túnel de IPsec. Por ejemplo, la tabla de ejemplo puede ser leída de manera que el tipo de usuario “HAP de GSM” está autorizado a utilizar un ancho de banda de 200 Kbits/segundo.

El propio “tipo de usuario” proporciona cierta información acerca de cómo deben actuar los nodos. Otra información por tipo de usuario puede ser relacionada, por ejemplo, para ajustes de seguridad. Ajustes de ejemplo para el GANC 13 se muestran en la Tabla 2 que sigue. Estos ejemplos definen limitaciones para cada registro de GAN en el GANC. Por ejemplo, la tabla de ejemplo puede ser leída de manera que el tipo de usuario “HAP de GSM” esté autorizado a enviar 200 mensajes por segundo.

Tabla 2

Tipo de Usuario	Mensajes permitidos por segundo	...
Por defecto	20	
HAP de GSM	200	
HAP de WCDMA	1000	
...		

La FIG. 13 es un diagrama de señalización que ilustra una extensión de la FIG. 12 para implementar la configuración basada en HLR para informar a la SEGW 14 de diferentes Tipos de usuario. Una nueva indicación de “Tipo de usuario” 91 es creada en el HSS/HLR 26 y devuelta al servidor de AAA 25 junto con la información de seguridad en la etapa 10. La información del “Tipo de Usuario” 91 puede estar basada en una IMSI individual o en un número de serie de IMSI asociado. También son posibles métodos de creación de indicación de “Tipo de Usuario” distintos de las variaciones del número de serie de IMSI. El servidor de AAA devuelve a continuación la información del “Tipo de Usuario” a la SEGW en la etapa 17 y la SEGW utiliza esta información para diferenciar entre diferentes tipos de usuario.

La FIG. 14 es un diagrama de señalización que ilustra una extensión de la FIG. 12 para implementar la configuración basada en AAA para informar a la SEGW 14 de diferentes Tipos de usuario. En esta realización, la nueva indicación de “Tipo de usuario” 91 es creada en el servidor de AAA 25 en lugar de en el HLR/HSS 26. De nuevo, la indicación del Tipo de usuario puede estar basada en una IMSI individual o en un número de serie de IMSI asociado, aunque también son posibles otros métodos de creación de indicación de Tipo de usuario. El servidor de AAA devuelve a continuación la información de “Tipo de Usuario” a la SEGW 14 en la etapa 17 y la SEGW utiliza esta información para diferenciar entre diferentes tipos de usuario.

En la realización que utiliza una configuración basada en SEGW, la nueva indicación de “Tipo de usuario” 91 es creada en la SEGW 14 y, de nuevo, puede estar basada en una IMSI individual o en un número de serie de IMSI. La SEGW utiliza esta información para diferenciar entre diferentes tipos de usuario. Un inconveniente con este planteamiento sería la O&M requerida. Típicamente existiría un número de SEGWs (distribuidas), y todas ellas necesitarían ser configuradas con información del tipo de usuario asociada con diferentes IMSIs o números de serie de IMSI y deberían mantenerse actualizadas.

La FIG. 15 es un diagrama de señalización que ilustra una realización de la presente invención para proporcionar información del tipo de usuario al GANC 13. La FIG. 15 es un diagrama de señalización que ilustra una extensión del procedimiento de Registro de GAN de la FIG. 3 para implementar la realización en la cual la SEGW 14 proporciona la información del tipo de usuario al GANC. En la etapa 93, la SEGW obtiene la indicación del Tipo de usuario 91

mediante una de las realizaciones anteriores. En la etapa 94, la SEGW proporciona la información del Tipo de usuario al GANC. El GANC utiliza entonces esta información para diferenciar entre diferentes tipos de usuario.

5 En otra realización de la presente invención, la nueva información de "Tipo de usuario" 91 es creada en el GANC 13 y, de nuevo, puede estar basada en una IMSI individual o en un número de serie de IMSI. El GANC utiliza esta información para diferenciar entre diferentes tipos de usuario. Un inconveniente con este planteamiento sería la O&M requerida. Típicamente existirían varios GANCs, y todos ellos necesitarían ser configurados con la información del tipo de usuario asociada con diferentes IMSIs o números de serie de IMSI y mantenidos actualizados.

10 En otra realización de la presente invención, la nueva indicación de "Tipo de usuario" es creada en una base de datos de la GAN que es accesible desde el GANC 13. El GANC pregunta a la base de datos de GAN durante el procedimiento de registro de GAN de la FIG. 3. De nuevo, la indicación del tipo de usuario puede estar basada en una IMSI individual o en un número de serie de IMSI asociado. El GANC utiliza a continuación esta información para diferenciar entre diferentes tipos de usuario.

15 Aunque se han ilustrado realizaciones preferidas de la presente invención en los dibujos que se acompañan y se han descrito en la Descripción Detallada anterior, debe comprenderse que la invención no está limitada a las realizaciones descritas, sino que es capaz de numerosas redistribuciones, modificaciones y sustituciones sin separarse del alcance de la invención. Por ejemplo, aunque las realizaciones de ejemplo descritas en esta memoria utilizaban la red de acceso de tipo Femto para GSM de GAN de las FIGs. 7 y 8, la invención puede ser también implementada utilizando la red de acceso de tipo Femto de WCDMA de GAN de las FIGS. 9 y 10. La memoria contempla cualquiera y todas las modificaciones que se encuentran dentro del alcance de la invención definida por
20 las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método en una red de acceso inalámbrica para proporcionar una indicación del tipo de usuario a una Puerta de Enlace de Seguridad, SEGW, durante un procedimiento de registro para un usuario, comprendiendo el citado método las etapas de:
- 5 recibir en un servidor de Autenticación, Autorización y Registro de Operaciones, AAA, una solicitud de autenticación del usuario;
- enviar una indicación del tipo de usuario para el usuario desde el servidor de AAA a la SEGW con un mensaje de éxito de autenticación, donde la información del tipo de usuario indica un tipo de túnel de IPsec; y
- 10 utilizar la indicación del tipo de usuario recibida en la SEGW para seleccionar y aplicar políticas asociadas al túnel de IPsec.
2. El método de acuerdo con lo citado en la reivindicación 1, en el que la etapa de enviar la indicación del tipo de usuario a la SEGW incluye crear la indicación del tipo de usuario en el servidor de AAA.
3. El método de acuerdo con lo citado en la reivindicación 2, en el que la etapa de creación de la indicación del tipo de usuario en el servidor de AAA incluye crear la indicación del tipo de usuario basándose en la Identidad de Estación de Telefonía Móvil Internacional, IMSI (International Mobile Station Identity, en inglés) del usuario, o en un número de serie de IMSI asociada.
- 15 4. El método de acuerdo con lo citado en la reivindicación 1, que comprende también enviar la indicación del tipo de usuario desde la SEGW a un Controlador de Red de Acceso Genérica, GANC (Generic Access Network Controller, en inglés).
- 20 5. El método de acuerdo con lo citado en la reivindicación 1, en el que la etapa de enviar la indicación del tipo de usuario a la SEGW incluye las etapas de:
- enviar una solicitud desde el servidor de AAA a un Registro de Ubicación Local, HLR (Home Local Register, en inglés), solicitando la información de autenticación para el usuario;
- crear la indicación del tipo de usuario en el HLR;
- 25 enviar una respuesta al servidor de AAA conteniendo la información de autenticación solicitada y la indicación del tipo de usuario para el usuario; y
- enviar la indicación del tipo de usuario desde el servidor de AAA a la SEGW.
- 30 6. El método de acuerdo con lo citado en la reivindicación 1, en el que la etapa de utilizar la indicación del tipo de usuario recibida en la SEGW para seleccionar y aplicar políticas asociadas al túnel de IPsec incluye situar limitaciones permitidas en el túnel de IPsec, siendo las citadas limitaciones seleccionadas de un grupo que consiste en ancho de banda permitido, número de conexiones de TCP permitidas, protocolo permitido, puertos de protocolo de destino permitidos, número de asociaciones de seguridad de IPsec permitidas y paquetes por segundo permitidos.
- 35 7. Un método para determinar la información del tipo de usuario en una Puerta de Enlace de Seguridad, SEGW (SEcurity GateWay, en inglés), en una red de acceso inalámbrica durante un procedimiento de registro para un usuario, comprendiendo el citado método las etapas de:
- almacenar en la SEGW, una base de datos que asocia diferentes Identidades de Estación de Telefonía Móvil Internacional, IMSIs (International Mobile Station Identities, en inglés), o números de serie con información del tipo de usuario indicando un tipo de túnel de IPsec;
- 40 recibir la IMSI del usuario en la SEGW durante el procedimiento del registro;
- determinar la información del tipo de usuario para el usuario basándose en la IMSI del usuario o en un número de serie de IMSI asociado; y
- utilizar la información del tipo de usuario determinada en la SEGW para seleccionar y aplicar políticas asociadas al túnel de IPsec.
- 45 8. El método de acuerdo con lo citado en la reivindicación 7, en el que la etapa de utilizar la información del tipo de usuario determinada en la SEGW para seleccionar y aplicar políticas asociadas al túnel de IPsec incluye disponer limitaciones permitidas en el túnel de IPsec, siendo las citadas limitaciones seleccionadas de un grupo consistente en ancho de banda permitido, número de conexiones de TCP permitidas, número de flujos de UDP permitidos, direcciones de IP de destino permitidas, protocolo permitido, puertos de protocolo de destino permitidos, número de asociaciones de seguridad de IPsec permitidas y paquetes por segundo permitidos.
- 50

9. Un método en una red de acceso inalámbrica para obtener información del tipo de usuario por parte de un nodo controlador durante un procedimiento de registro para un usuario, comprendiendo el citado método las etapas de:
- 5 configurar una base de datos con la información del tipo de usuario asociada con diferentes Identidades de Estación de Telefonía Móvil Internacional, IMSIs, o número de serie de IMSI, donde la información del tipo de usuario indica un tipo de túnel de IPsec,
- recibir la IMSI del usuario en el nodo controlador durante el procedimiento de registro; y
- utilizar la IMSI del usuario por parte del nodo controlador para obtener la información del tipo de usuario para el usuario a partir de la base de datos.
10. Un método en una red de acceso inalámbrica para determinar la información del tipo de usuario en un nodo controlador durante un procedimiento de registro para un usuario, comprendiendo el citado método las etapas de:
- configurar el nodo controlador con la información del tipo de usuario asociada con diferentes Identidades de Estación de Telefonía Móvil Internacional, IMSIs (International Mobile Station Identities, en inglés), o número de serie de IMSI, donde la información del tipo de usuario indica un tipo de túnel de IPsec;
- recibir la IMSI del usuario en el nodo controlador durante el procedimiento de registro; y
- 15 determinar la información del tipo de usuario por parte del nodo controlador basándose en la IMSI del usuario o en el número de serie de una IMSI asociada.
11. Un servidor de Autenticación, Autorización y Registro de Operaciones, AAA (Authentication, Authorization and Accounting, en inglés), para proporcionar una indicación del tipo de usuario a una Puerta de Enlace de Seguridad, SEGW (SEcurity GateWay, en inglés), durante un procedimiento de registro para un usuario, comprendiendo el
- 20 citado servidor de AAA:
- un medio para recibir una solicitud de autenticación del usuario; y
- un medio para enviar una indicación del tipo de usuario para el usuario a la SEGW con un mensaje de éxito de autenticación, en el que la indicación del tipo de usuario indica un tipo de túnel de IPsec;
- 25 en el que la SEGW utiliza la indicación del tipo de usuario recibida para seleccionar y aplicar políticas asociadas en el túnel de IPsec.
12. El servidor de AAA de acuerdo con lo citado en la reivindicación 11, en el que el medio para enviar la indicación del tipo de usuario a la SEGW incluye un medio para crear la indicación del tipo de usuario en el servidor de AAA.
13. El servidor de AAA de acuerdo con lo citado en la reivindicación 12, en el que el medio para crear la indicación del tipo de usuario en el servidor de AAA incluye un medio para crear la indicación del tipo de usuario basándose en
- 30 la Identidad de Estación de Telefonía Móvil Internacional, IMSI (International Mobile Station Identity, en inglés), o un número de serie de IMSI asociado.
14. El servidor de AAA de acuerdo con lo citado en la reivindicación 11, en el que el medio para enviar la indicación del tipo de usuario a la SEGW incluye:
- 35 un medio para enviar una solicitud desde el servidor de AAA a un Registro de Ubicación Local, HLR (Home Location Register, en inglés), solicitando información de autenticación para el usuario;
- un medio para recibir una respuesta desde el HLR conteniendo la información de autenticación solicitada y la indicación del tipo de usuario para el usuario; y
- un medio para enviar la indicación del tipo de usuario desde el servidor de AAA a la SEGW.
- 40 15. Un aparato en una Puerta de Enlace de Seguridad, SEGW, (SEcurity GateWay, en inglés), en una red de acceso, comprendiendo el citado aparato:
- una base de datos configurada para asociar información del tipo de usuario con diferentes Identidades de Estación de Telefonía Móvil Internacional, IMSIs (International Mobile Station Identities, en inglés), o un número de serie de IMSI asociado, donde la información del tipo de usuario indica un tipo de túnel de IPsec;
- un medio para recibir la IMSI de un usuario durante un procedimiento de registro;
- 45 un medio para determinar la información del tipo de usuario para el usuario basándose en la IMSI del usuario o en el número de serie de una IMSI asociada; y
- un medio para utilizar la información del tipo de usuario determinada en la SEGW para seleccionar y aplicar políticas asociadas al túnel de IPsec.

- 5 16. El aparato de acuerdo con lo citado en la reivindicación 15, en el que el medio para utilizar la información del tipo de usuario determinada en la SEGW para seleccionar y aplicar políticas asociadas al túnel de IPsec está adaptado para disponer limitaciones permitidas en el túnel de IPsec, estando las citadas limitaciones seleccionadas de un grupo que consiste en ancho de banda permitido, número de conexiones de TCP permitidas, número de flujos de UDP permitidos, direcciones de IP de destino permitidas, protocolo permitido, puertos de protocolo de destino permitidos, número de asociaciones de seguridad de IPsec permitidas y paquetes por segundo permitidos.
17. Un sistema en una red de acceso para proporcionar información del tipo de usuario a un nodo controlador durante un procedimiento de registro para un usuario, comprendiendo el citado sistema:
- 10 una base de datos configurada para asociar la información del tipo de usuario con diferentes Identidades de Estación de Telefonía Móvil Internacional, IMSIs (International Mobile Station Identities, en inglés), o número de serie de IMSI, donde la información del tipo de usuario indica un tipo de túnel de IPsec;
- un medio dentro del nodo controlador para recibir la IMSI del usuario durante un procedimiento de registro; y
- un medio dentro del nodo controlador para utilizar la IMSI del medio con el fin de obtener la información del tipo de usuario para el usuario a partir de la base de datos.
- 15 18. Un aparato en un nodo controlador en una red de acceso, comprendiendo el citado aparato:
- una base de datos configurada para asociar la información del tipo de usuario con diferentes Identidades de Estación de Telefonía Móvil Internacional, IMSIs (International Mobile Station Identities, en inglés), o número de serie de IMSI, donde la información del tipo de usuario indica un tipo de túnel de IPsec;
- un medio para recibir la IMSI de un usuario durante un procedimiento de registro; y
- 20 un medio para determinar la información del tipo de usuario para el usuario basándose en la IMSI del usuario o en el número de serie de una IMSI asociada.
- 25 19. Un método en una Puerta de Enlace de Seguridad, SEGW, (SEcurity GateWay, en inglés), en una red de acceso inalámbrica para seleccionar y aplicar políticas a un túnel de IPsec durante un procedimiento de registro para un usuario en el cual un servidor de Autenticación, Autorización y Registro de Operaciones, AAA (Authentication, Authorization and Accounting, en inglés), recibe una solicitud de autenticación del usuario, comprendiendo el citado método las etapas de:
- recibir desde el servidor de AAA, un mensaje de éxito de autenticación incluyendo una información del tipo de usuario para el usuario, donde la indicación del tipo de usuario indica un tipo de túnel de IPsec; y
- 30 utilizar la indicación del tipo de usuario recibida en la SEGW para seleccionar y aplicar políticas asociadas al túnel de IPsec.

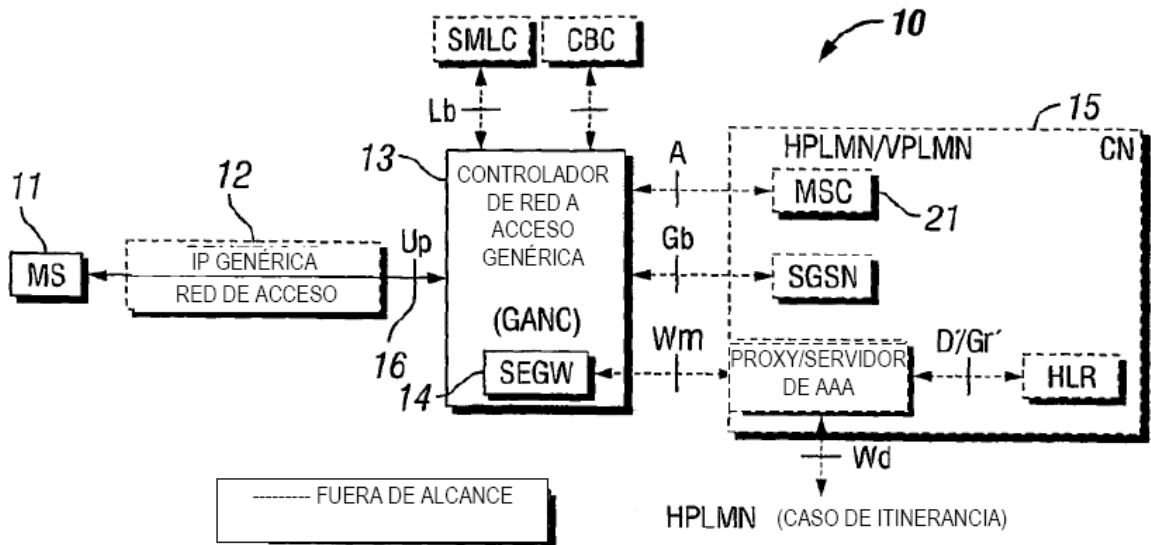


FIG. 1
(Técnica Anterior)

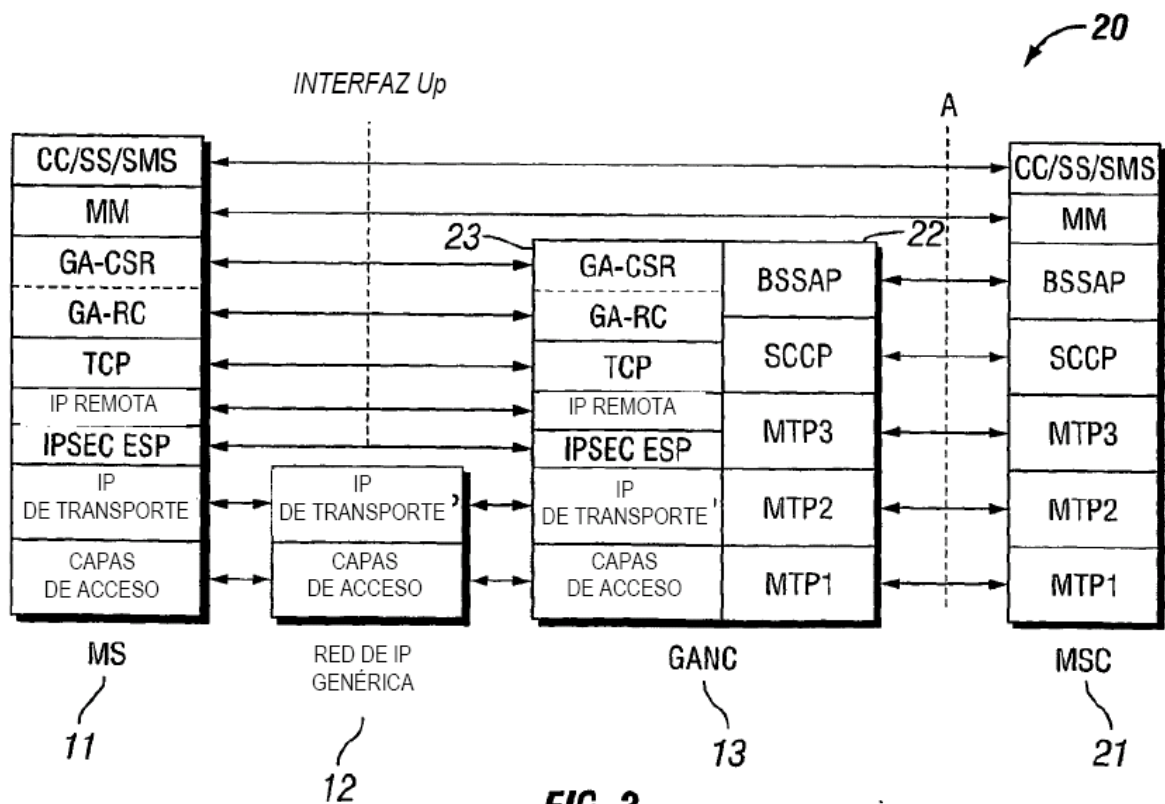


FIG. 2
(Técnica Anterior)

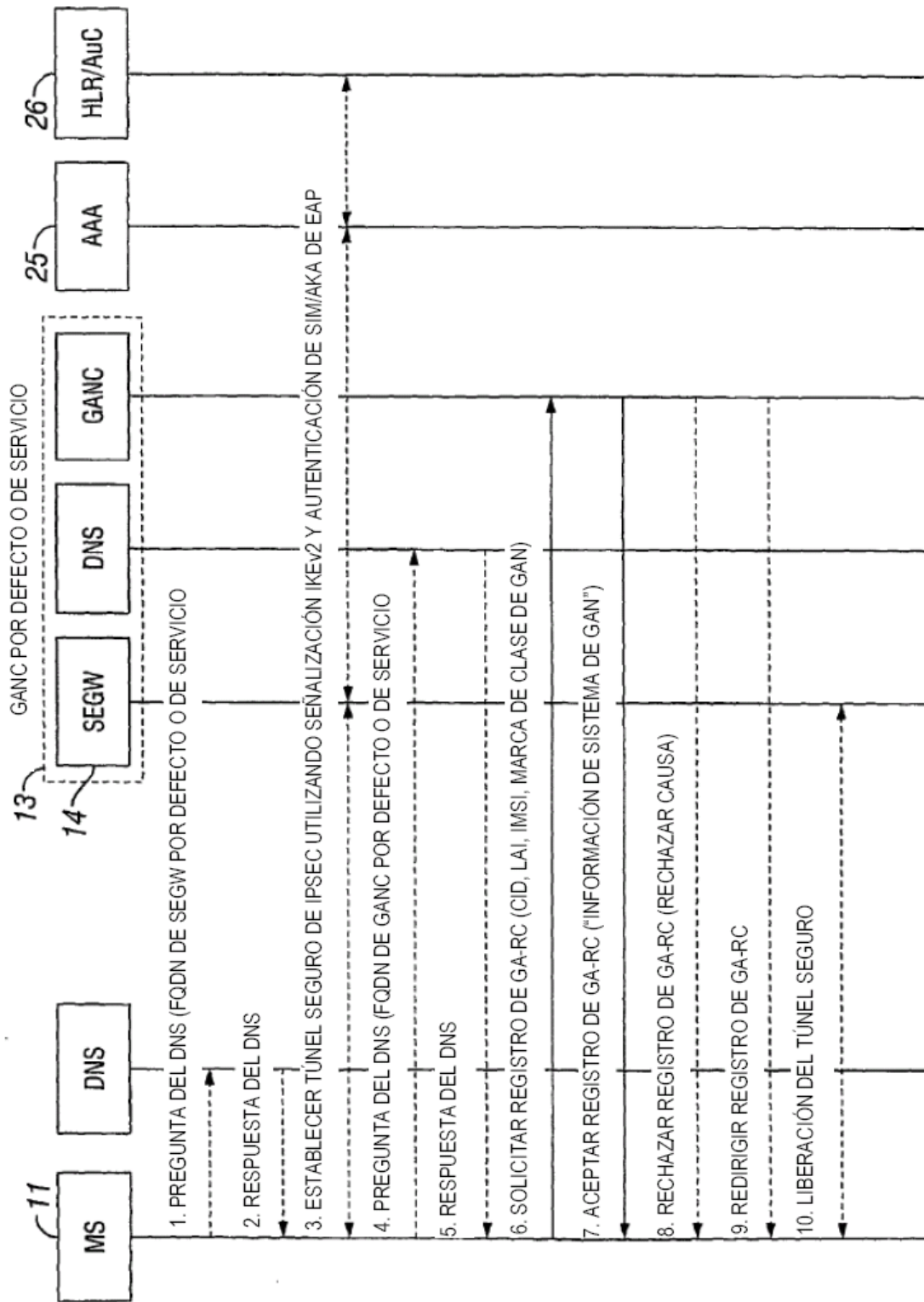


FIG. 3
(Técnica Anterior)

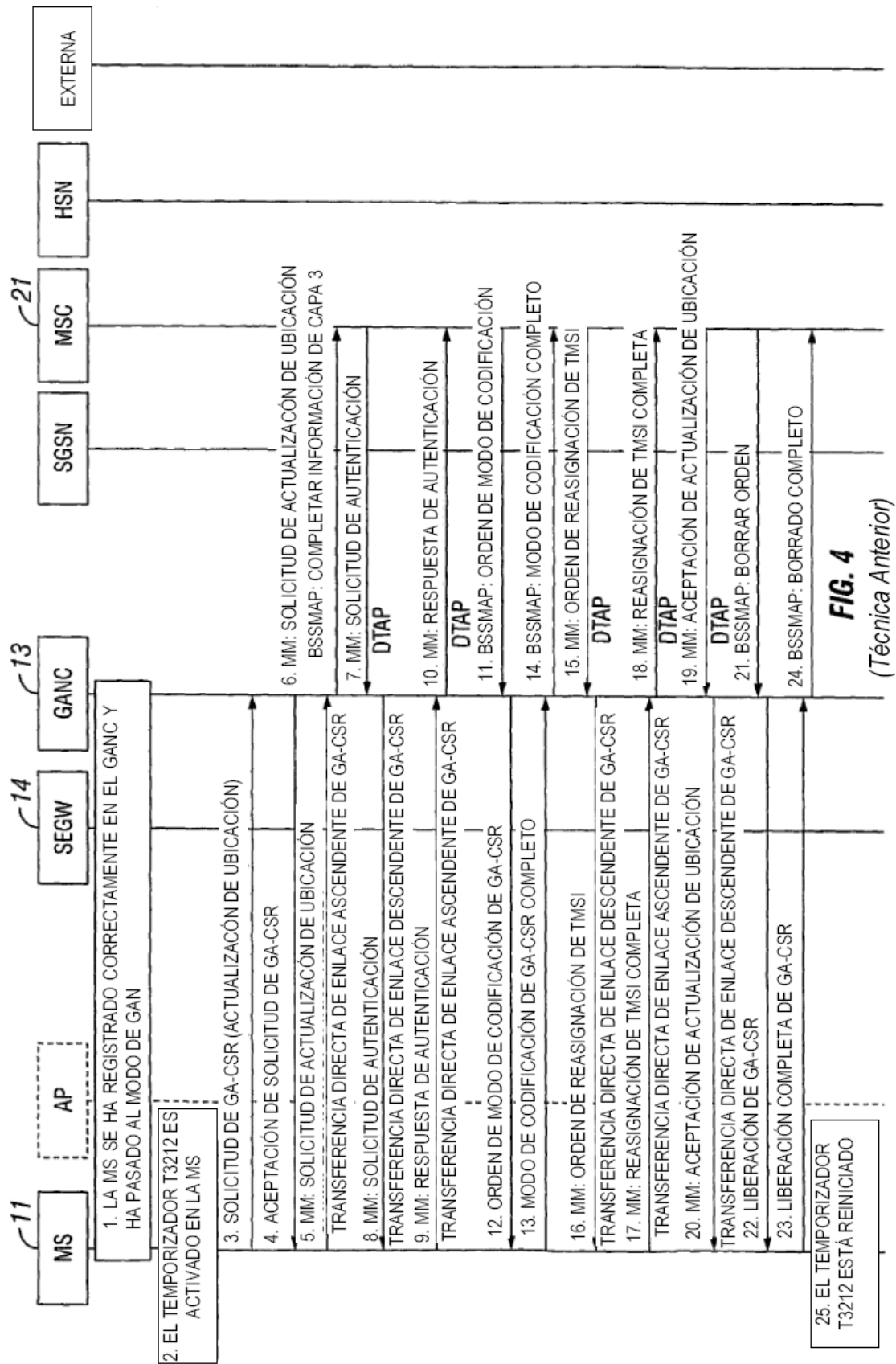


FIG. 4
(Técnica Anterior)

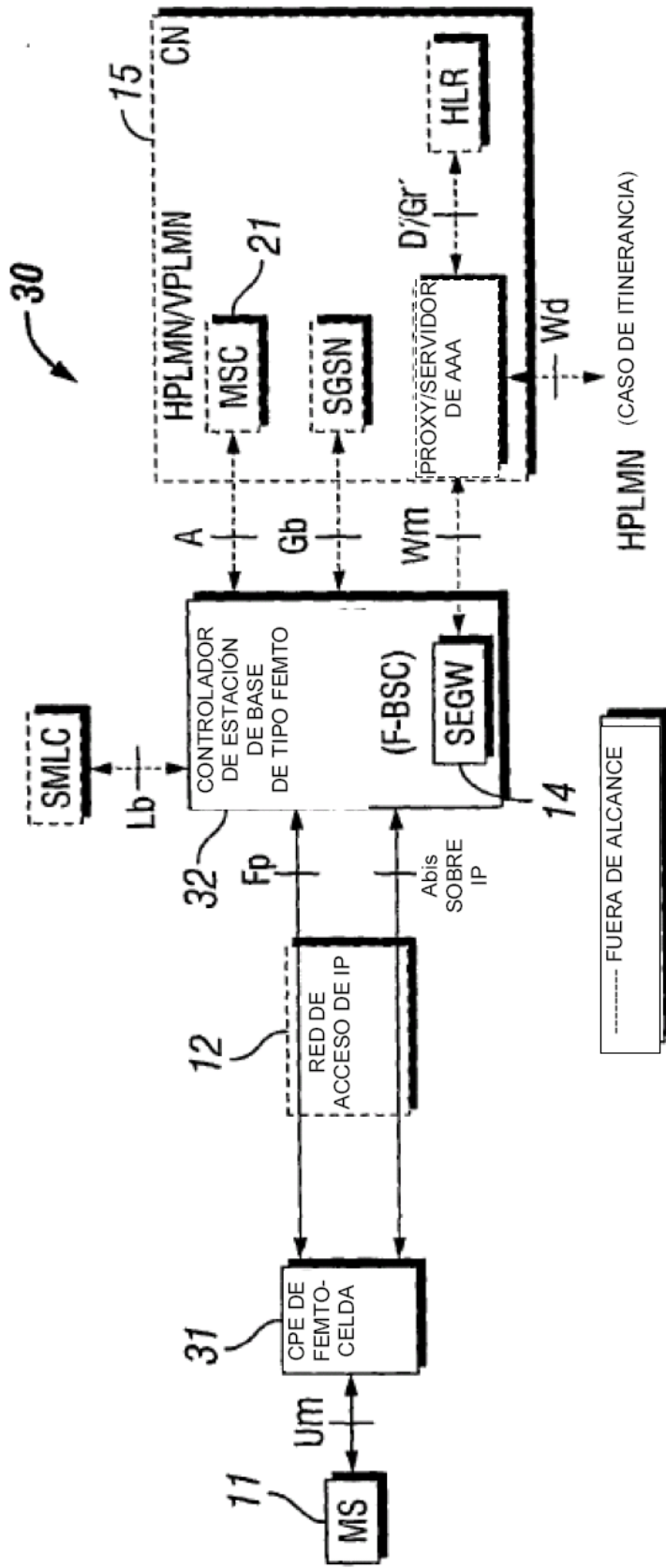


FIG. 5
(Técnica Anterior)

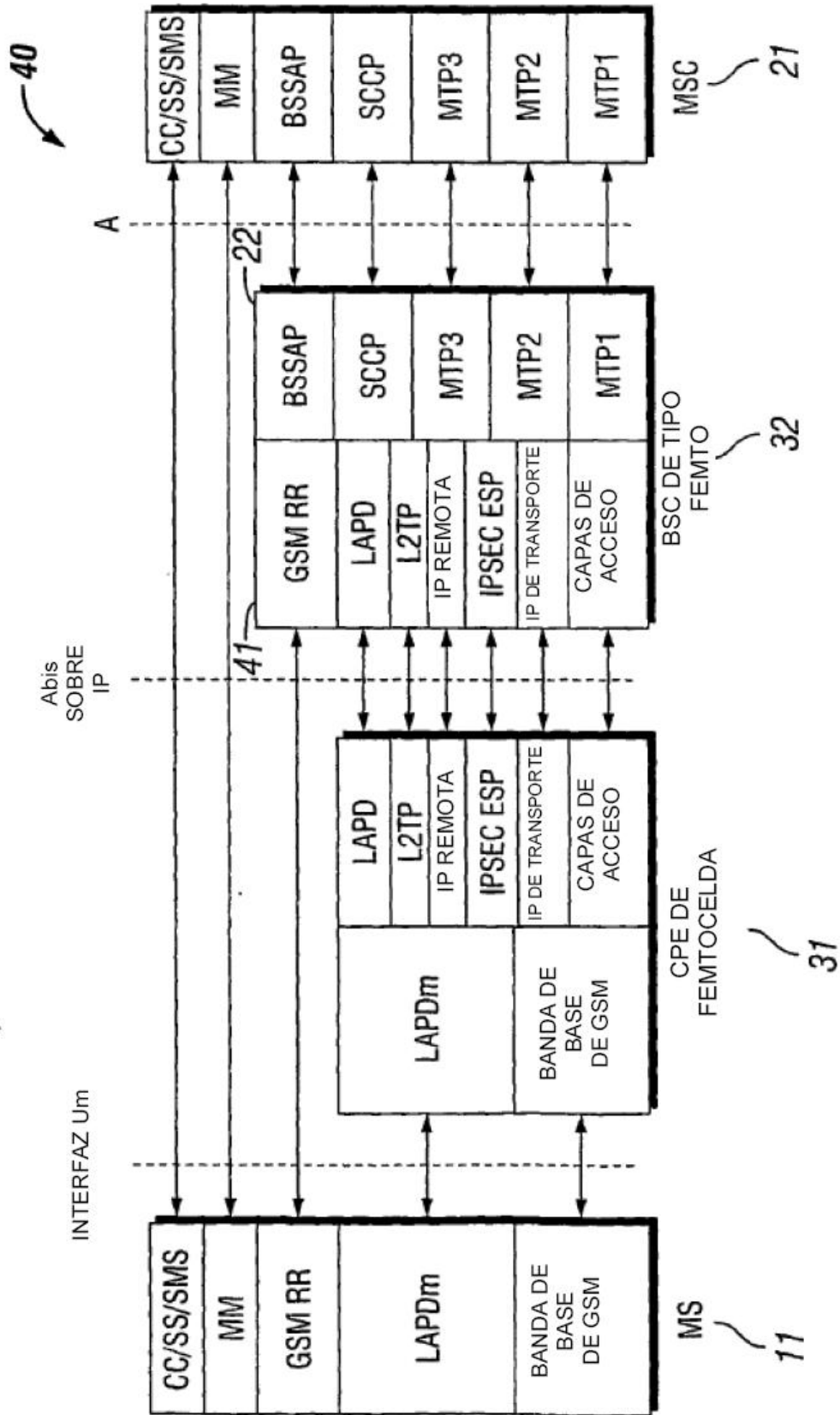


FIG. 6
(Técnica Anterior)

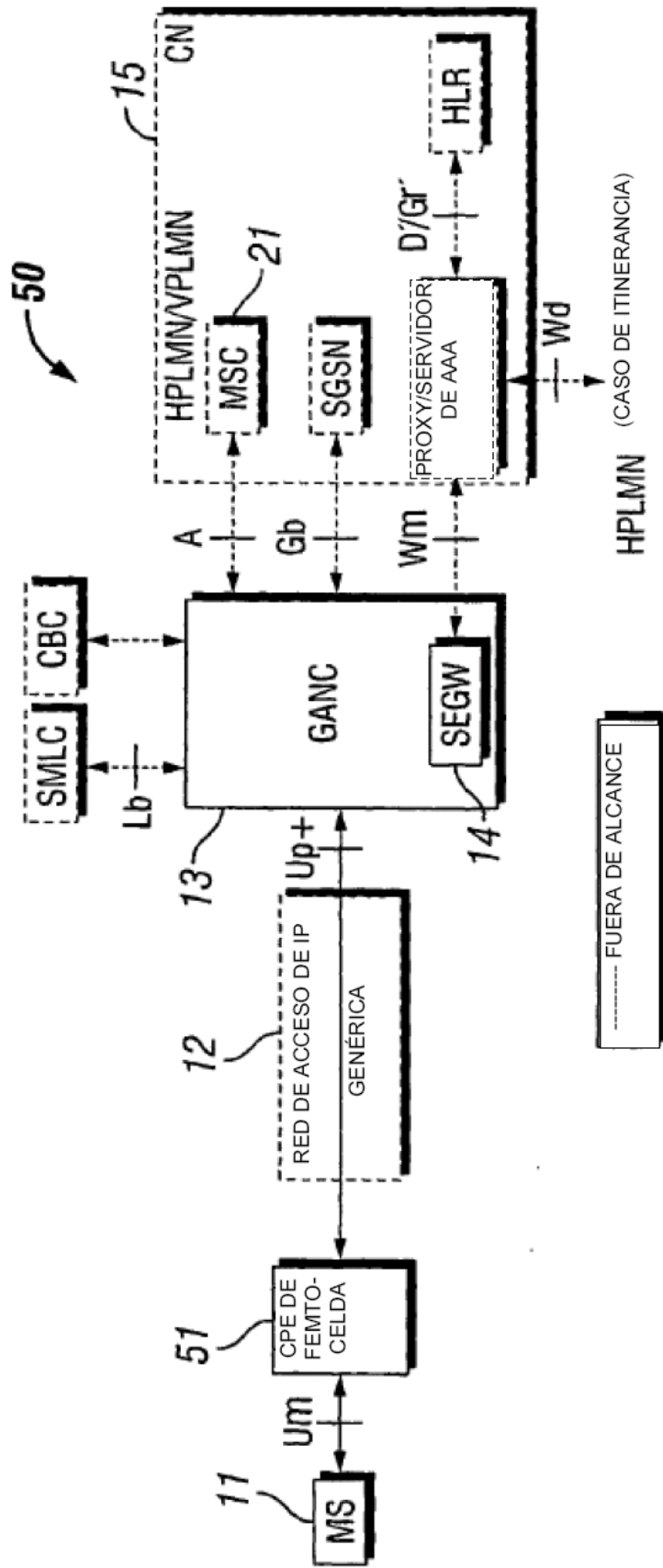


FIG. 7

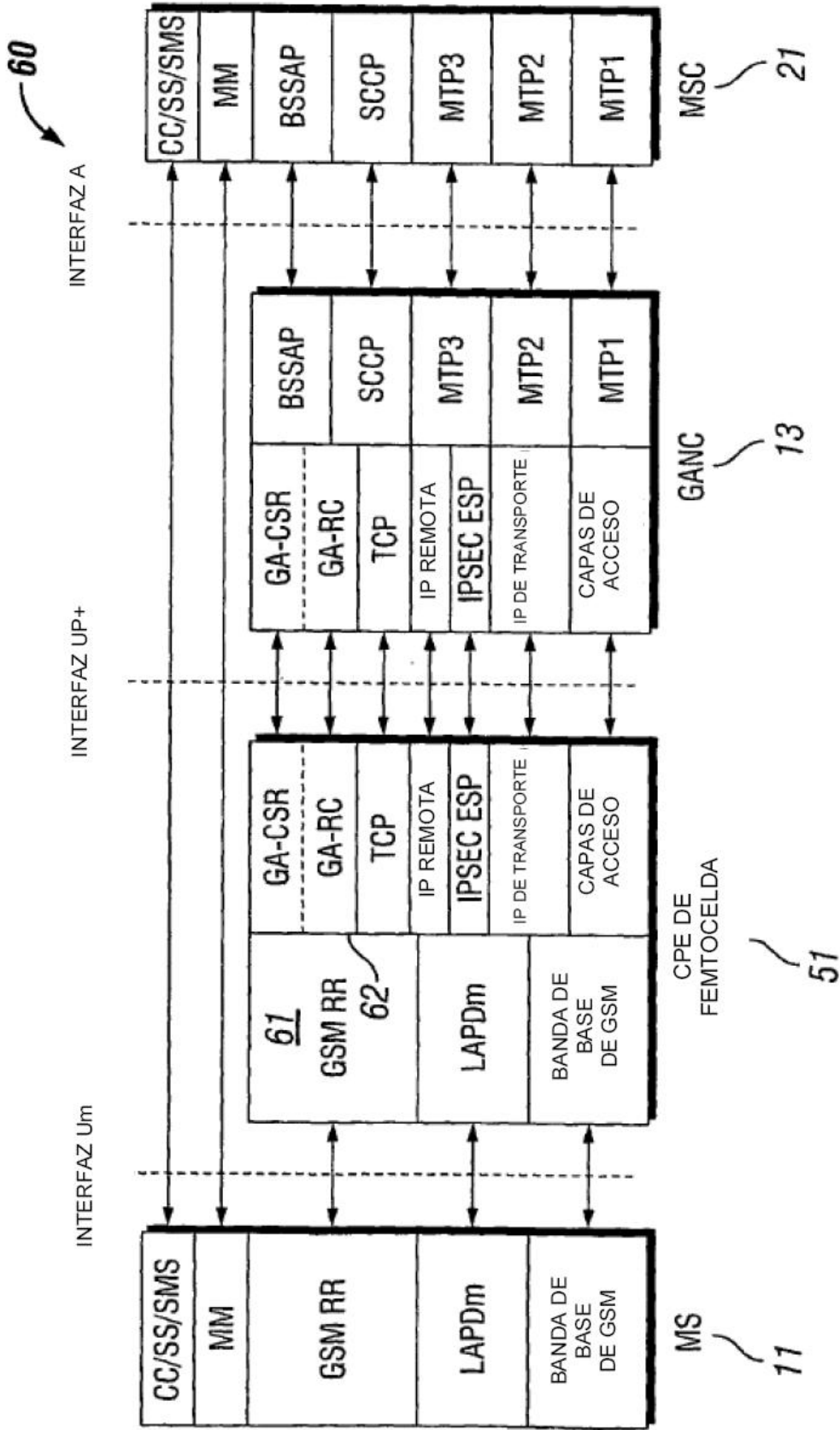


FIG. 8

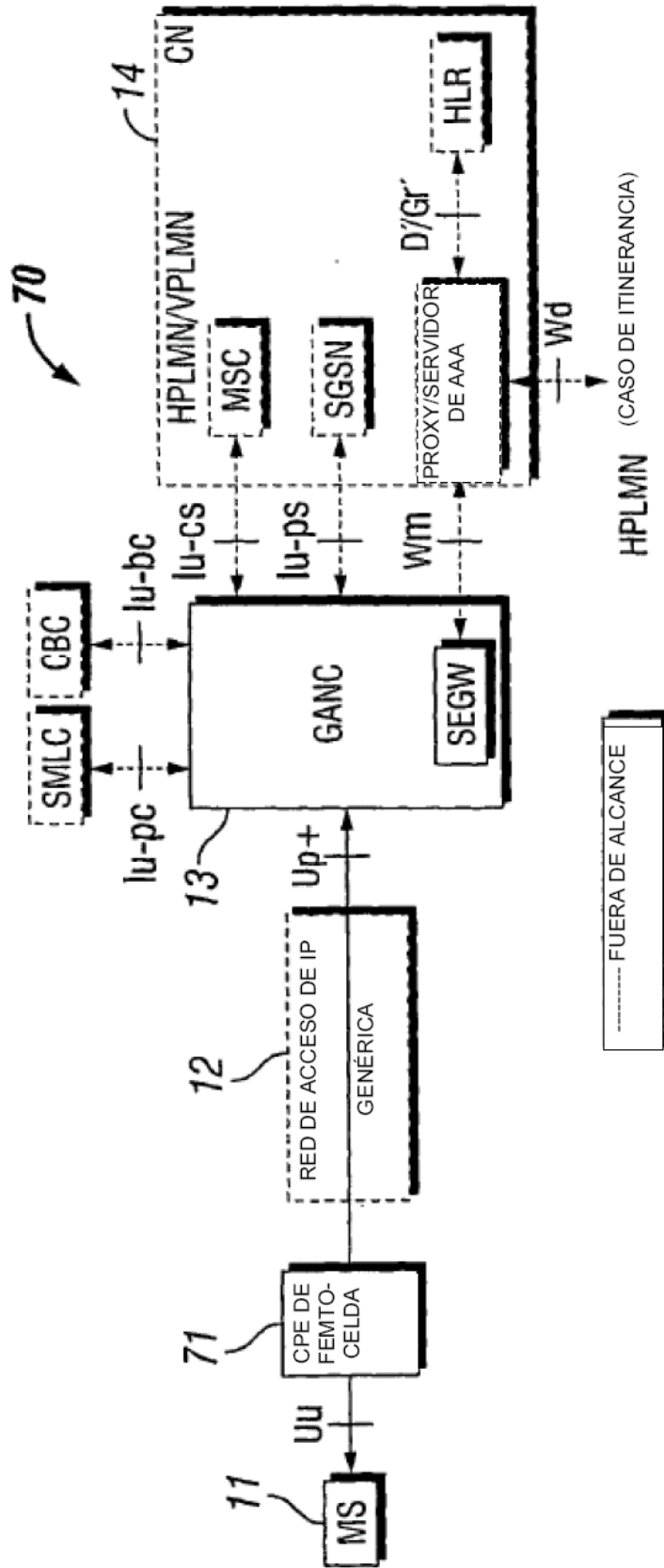


FIG. 9

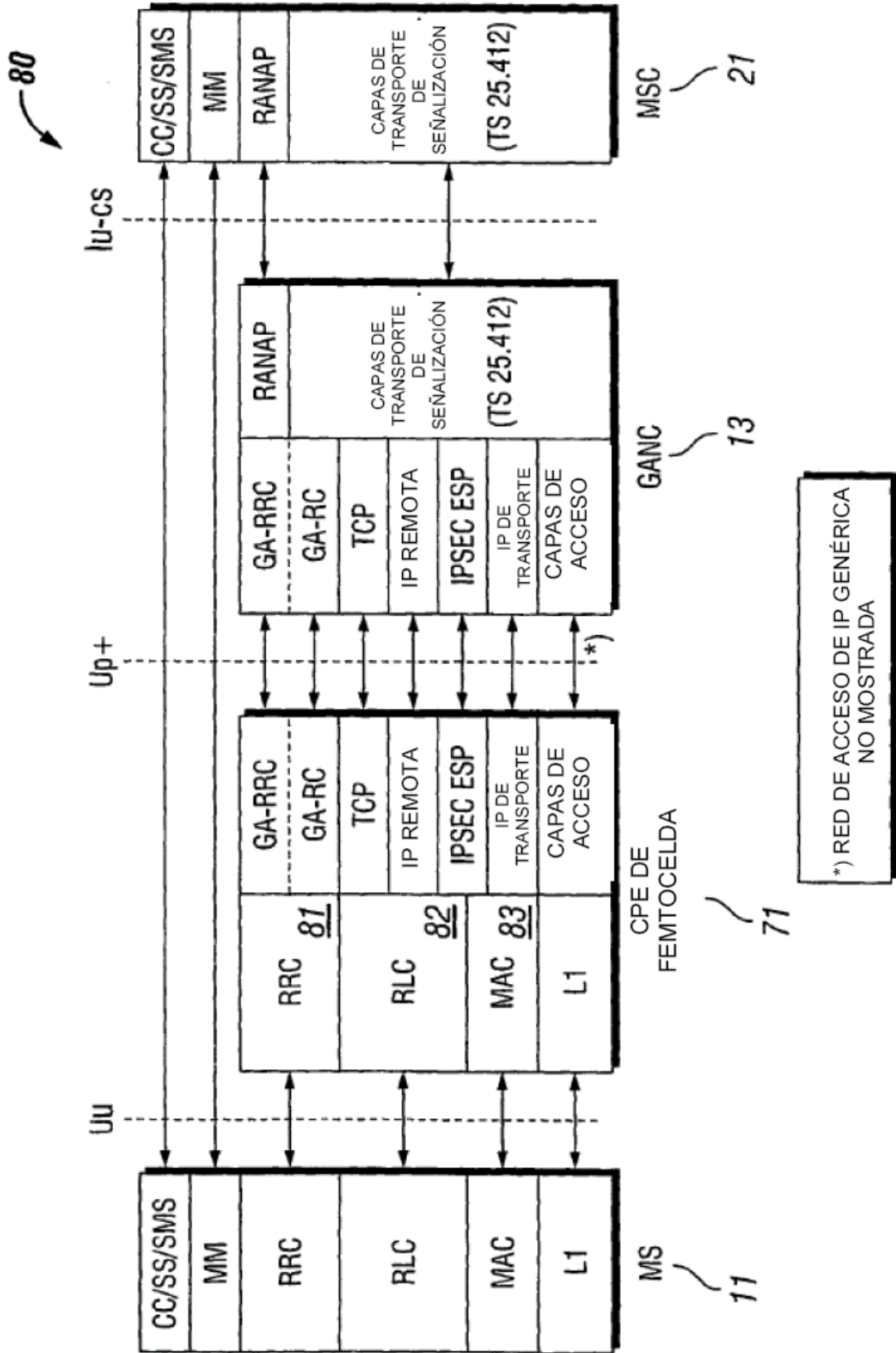


FIG. 10

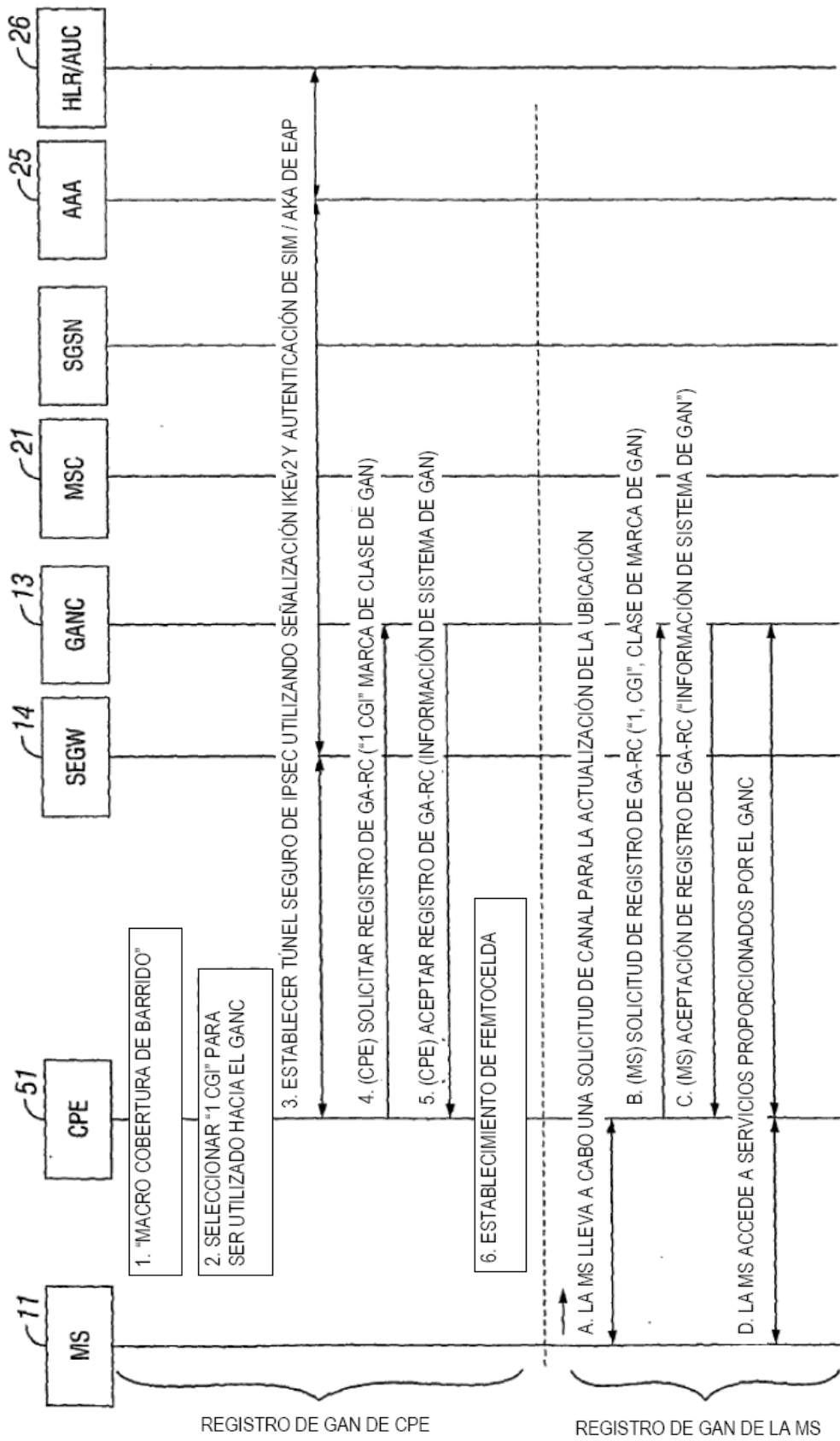


FIG. 11

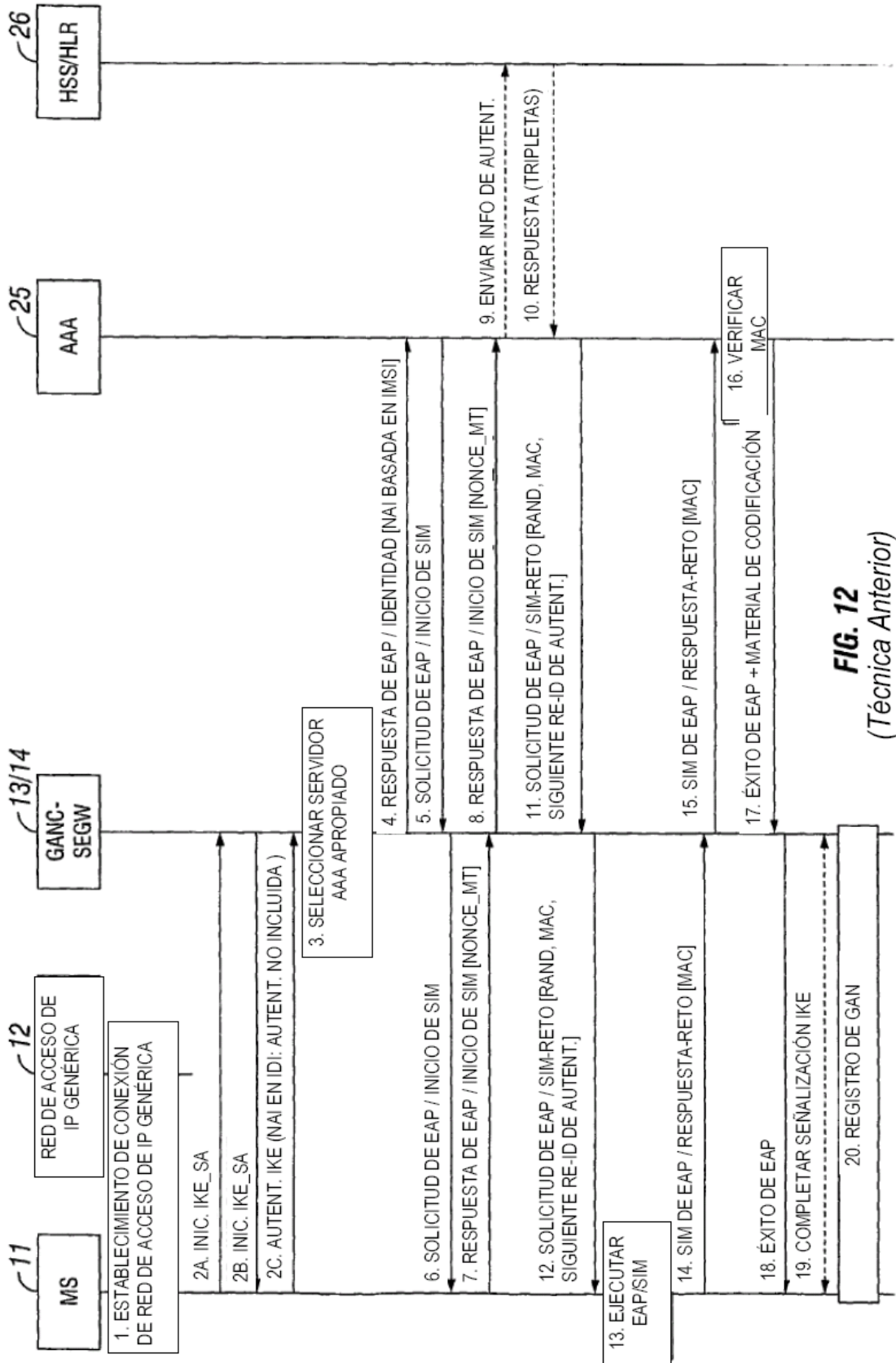


FIG. 12
(Técnica Anterior)

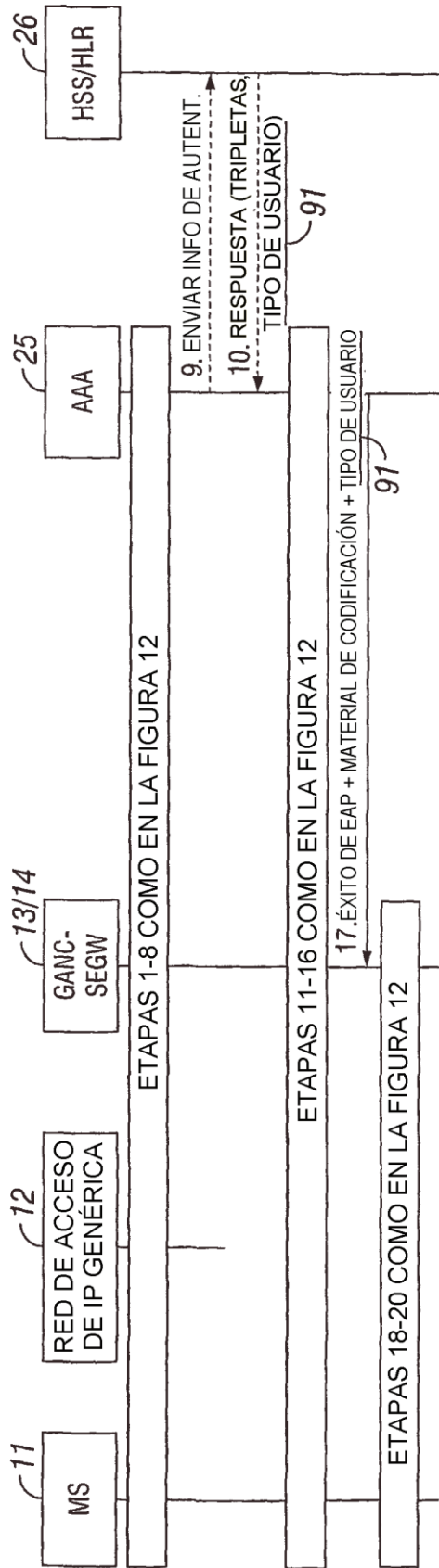


FIG. 13

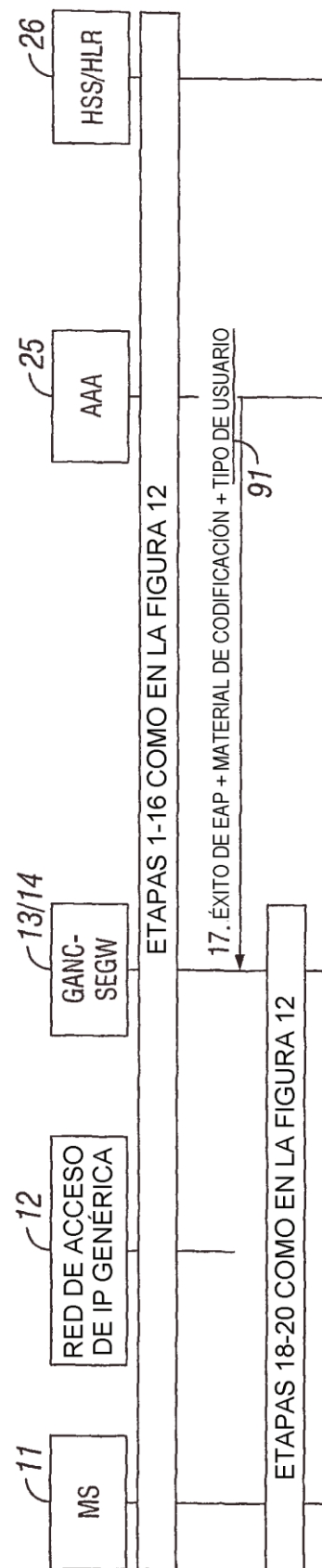


FIG. 14

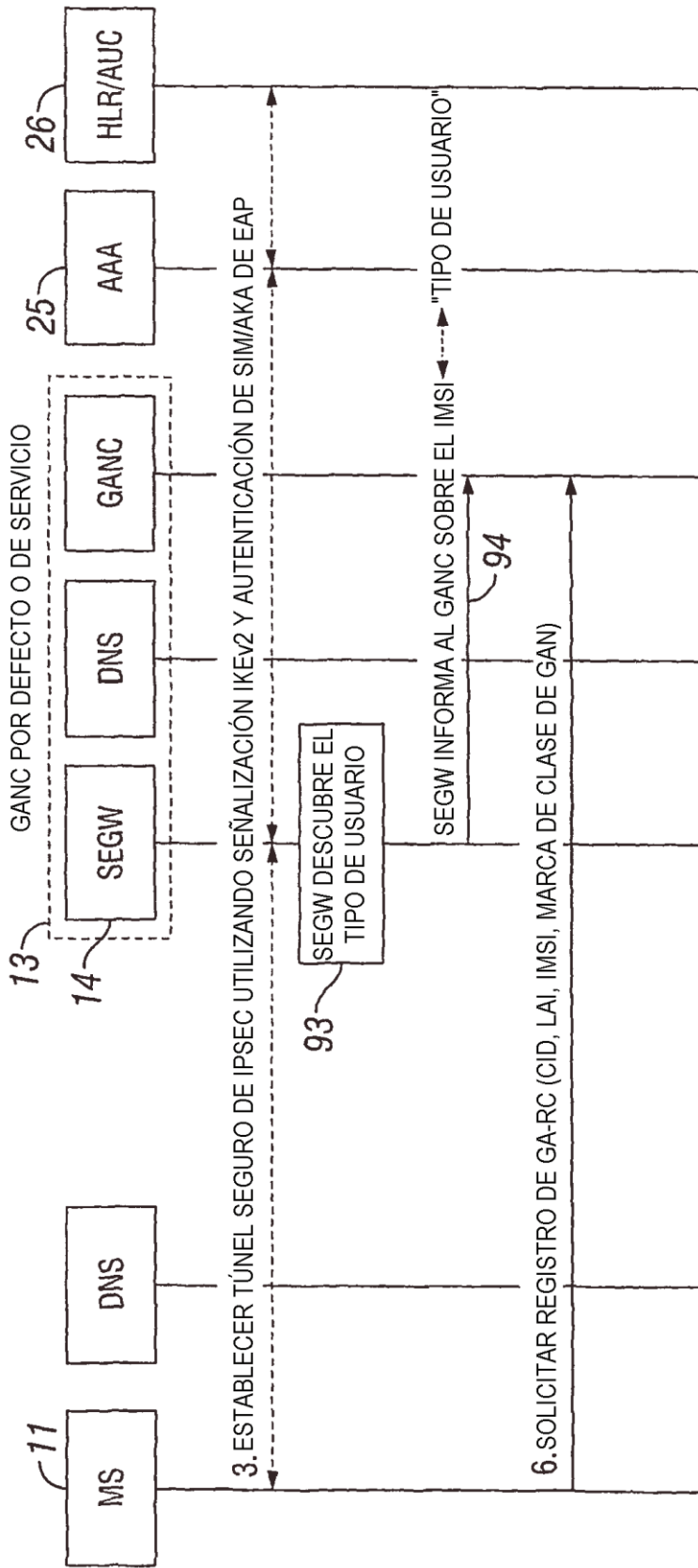


FIG. 15