(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 681 679**

(51) Int. CI.:

H04M 3/42 (2006.01)
H04L 29/06 (2006.01)
H04W 4/90 (2008.01)
H04M 1/725 (2006.01)
H04M 1/253 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.08.2006 PCT/US2006/030349**

(87) Fecha y número de publicación internacional: **08.02.2007 WO07016695**

(96) Fecha de presentación y número de la solicitud europea: **02.08.2006 E 06789352 (9)**

(97) Fecha y número de publicación de la concesión europea: **06.06.2018 EP 1911257**

(54) Título: **Admisión de llamadas de emergencia VoIP**

(30) Prioridad:

02.08.2005 US 704977 P
30.08.2005 US 713199 P
13.10.2005 US 726694 P
31.10.2005 US 732226 P
09.12.2005 US 748821 P
01.08.2006 US 497703

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.09.2018

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121, US

(72) Inventor/es:

EDGE, STEPHEN;
BURROUGHS, KIRK y
NASIELSKI, JOHN

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Admisión de llamadas de emergencia VoIP

ANTECEDENTES

1.1. Campo

[1] La presente divulgación se refiere, en general, a la comunicación, y más específicamente a técnicas para admitir llamadas de emergencia.

1.2. Antecedentes

[2] Las redes de comunicación inalámbrica están ampliamente implantadas para proporcionar diversos servicios de comunicación, como voz, vídeo, paquetes de datos, mensajería, radiodifusión, etc. Estas redes inalámbricas pueden ser redes de acceso múltiple capaces de admitir comunicaciones para múltiples usuarios al compartir los recursos de red disponibles. Ejemplos de dichas redes de acceso múltiple incluyen redes de acceso múltiple por división de código (CDMA), redes de acceso múltiple por división de tiempo (TDMA), redes de acceso múltiple por división de frecuencia (FDMA) y redes FDMA ortogonales (OFDMA).

[3] Las redes inalámbricas típicamente admiten comunicaciones para usuarios inalámbricos que tienen suscripciones de servicio con estas redes. Una suscripción de servicio puede estar asociada a información de seguridad, encaminamiento, calidad de servicio (QoS), facturación, etc. La información relacionada con la suscripción se puede usar para establecer llamadas con una red [network] inalámbrica.

[4] Uno de los servicios más básicos que proporcionan las redes inalámbricas para sus usuarios es la capacidad de enviar y recibir llamadas de voz. Una mejora reciente de este servicio es la capacidad de enviar y recibir llamadas de Voz sobre Protocolo de Internet (VoIP). Una llamada VoIP es una llamada de voz en la que los datos de voz se envían en paquetes que se encaminan como otros datos de paquete en lugar de en un canal de tráfico dedicado.

[5] Un usuario inalámbrico puede hacer una llamada de emergencia u otra llamada de medios con una red inalámbrica que puede o no ser una red doméstica con la cual el usuario tiene suscripción de servicio. Dicha llamada puede usar VoIP. Un desafío importante es encaminar la llamada de emergencia a un punto de respuesta de seguridad pública (PSAP) apropiado que pueda atender la llamada. Esto puede implicar obtener una estimación de posición provisional para el usuario y determinar el PSAP adecuado en base a la estimación de la posición provisional. El problema se agrava si el usuario está en itinerancia y/o no tiene suscripción de servicio con ninguna red.

[6] Por lo tanto, existe una necesidad en la técnica de técnicas para admitir llamadas de emergencia y llamadas de VoIP de emergencia.

[7] Se llama la atención sobre el documento WO 02/03718 A2 que se refiere a una llamada telefónica de emergencia que es admitida y encaminada a un punto de respuesta de seguridad pública (PAP) en una red de comunicaciones inalámbricas conmutadas por paquetes basada en IP. Una solicitud de activar el contexto PDP se envía desde un equipo de usuario a la red. Un parámetro en dicha solicitud de activar el contexto PDP indica que el contexto PDP se usará para transferir una llamada de emergencia. Se devuelve un mensaje de aceptación de la activación del contexto PDP desde dicho nodo de soporte a dicho equipo de usuario. Dicho mensaje de aceptación de la activación del contexto PDP acusa el recibo de dicho mensaje de solicitud de activación del contexto PDP y proporciona la dirección de una función de control de estado de la llamada. Una solicitud de configuración de llamada transferida a la función de control de estado de la llamada incluye la identidad del área de servicio (SAI). La función de control de estado de la llamada selecciona un PSAP basándose, al menos en parte, en la SAI incluida en la solicitud de configuración de llamada y reenvía la llamada de emergencia al PSAP seleccionado.

[8] Se centra más la atención en el documento EP 1 526 697 A2 que se refiere a proporcionar servicios de emergencia mejorados (E-911) a una PBX basada en telefonía IP o sistema similar, utilizando aspectos de la inteligencia de los dispositivos cliente SIP del usuario final para abordar desafíos y dificultades asociados con los servicios similares al E-911 en entornos de telefonía LAN.

SUMARIO

[9] De acuerdo con la presente invención, se proporcionan un procedimiento, según se expone en la reivindicación 1, y un equipo de usuario, según se expone en la reivindicación 4. Otros modos de realización se reivindican en las reivindicaciones dependientes.

[10] En el presente documento, se describen técnicas para admitir llamadas de emergencia de voz sobre protocolo de internet (VoIP). Las técnicas se pueden usar para diversas redes 3GPP y 3GPP2, diversas arquitecturas de ubicación y equipos de usuario (UE) con y sin suscripción de servicio.

[11] En un modo de realización, un UE se comunica con una red visitada para enviar una solicitud para establecer una llamada de VoIP de emergencia. El UE interactúa con un servidor de ubicación instruido por la red visitada para obtener una primera estimación de posición para el UE. El UE realiza la configuración de la llamada a través de la red visitada para establecer la llamada de VoIP de emergencia con un PSAP, que se puede seleccionar basándose en la estimación de la posición inicial. A continuación, el UE puede realizar el posicionamiento con el servidor de ubicación para obtener una estimación de posición actualizada para el UE, por ejemplo, si lo solicita el PSAP. Varios detalles de la llamada de VoIP de emergencia se describen a continuación.

[12] También se describen en más detalle diversos aspectos y modos de realización de la presente divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[13] Los aspectos y los modos de realización de la divulgación se harán más evidentes a partir de la descripción detallada que se expone a continuación cuando se toma junto con los dibujos en los que iguales caracteres de referencia se identifican correspondientemente en todos los dibujos.

La FIG. 1 muestra una implementación que admite llamadas de VoIP de emergencia.

La FIG. 2 muestra una arquitectura de red 3GPP.

La FIG. 3 muestra una arquitectura de red 3GPP2.

Las FIGs. 4 y 5 muestran una arquitectura de red y un flujo de mensajes, respectivamente, para llamadas de VoIP de emergencia con ubicación SUPL.

Las FIGs. 6 y 7 muestran una arquitectura de red y un flujo de mensajes, respectivamente, para llamadas de VoIP de emergencia con ubicación de plano de control 3GPP.

Las FIGs. 8 y 9 muestran una arquitectura de red y un flujo de mensajes, respectivamente, para llamadas de VoIP de emergencia con la ubicación X.S0024.

Las FIGs. 10 y 11 muestran una arquitectura de red y un flujo de mensajes, respectivamente, para llamadas de VoIP de emergencia para un UE sin suscripción de servicio.

La FIG. 12 muestra un diagrama de bloques de varias entidades de las FIGs. 1 a 3.

DESCRIPCIÓN DETALLADA

[14] Los términos "a modo de ejemplo" se usan en el presente documento en el sentido de "que sirve de ejemplo, caso o ilustración". No debe considerarse necesariamente que cualquier modo de realización o diseño descritos en el presente documento como "a modo de ejemplo" sean preferidos o ventajosos con respecto a otros modos de realización o diseños.

[15] Las técnicas para admitir llamadas de VoIP de emergencia se describen en el presente documento. Una llamada de VoIP de emergencia es una llamada de VoIP o una llamada de conmutación por paquetes para servicios de emergencia. Una llamada de VoIP de emergencia puede identificarse como tal y se puede distinguir de una llamada de VoIP normal de varias maneras, como se describe a continuación. Una llamada de VoIP de emergencia puede estar asociada con varias características que son diferentes de una llamada VoIP ordinaria, como, por ejemplo, obtener una estimación de posición adecuada para un usuario, encaminar la llamada de VoIP de emergencia a un PSAP apropiado, y así sucesivamente. Una estimación de posición también se conoce como estimación de ubicación, corrección de posición, etc.

[16] **La FIG. 1** muestra una implementación 100 que admite llamadas de VoIP de emergencia. Un Equipo de Usuario (UE) 110 se comunica con una red de acceso 120 para obtener servicios básicos de comunicación IP. El UE 110 puede ser estacionario o móvil y también se puede llamar una estación móvil (MS), un terminal, una unidad de abonado, una estación o alguna otra terminología. El UE 110 puede ser un teléfono celular, un asistente digital personal (PDA), un dispositivo inalámbrico, un ordenador portátil, un dispositivo de telemetría, un dispositivo de rastreo y así sucesivamente. El UE 110 puede comunicarse con una o más estaciones base y/o uno o más puntos de acceso en la red de acceso 120. El UE 110 también puede recibir señales desde uno o más satélites 190, que pueden ser parte del Sistema de Posicionamiento Global (GPS), el sistema europeo Galileo, el

sistema ruso GLONASS o cualquier Sistema Global de Navegación por Satélite (GNSS). El UE 110 puede medir señales desde estaciones base en la red de acceso 120 y/o señales de los satélites 190 y puede obtener mediciones de pseudodistancia para los satélites y/o mediciones de temporización para las estaciones base. Las mediciones de pseudodistancia y/o las mediciones de temporización pueden usarse para obtener una estimación de la posición para el UE 110 usando uno o una combinación de procedimientos de posicionamiento bien conocidos en la técnica tales como GPS asistido (A-GPS), GPS independiente, trilateración de enlace directo avanzado (A-FLT), diferencia de tiempo observada mejorada (E-OTD), diferencia de tiempo de llegada observada (OTDOA), ID de célula mejorada, etc.

[17] La red de acceso 120 proporciona comunicación por radio para los UE ubicados dentro del área de cobertura de la red de acceso. La red de acceso 120 puede incluir estaciones base, controladores de red y/u otras entidades, como se describe a continuación. Una red visitada 130, que también se denomina Red móvil terrestre pública visitada (V-PLMN), es una red que actualmente sirve al UE 110. Una red doméstica 160, que también se denomina PLMN doméstica (H-PLMN), es una red con la que el UE 110 tiene suscripción. La red de acceso 120 está asociada a la red visitada 130. La red visitada 130 y la red doméstica 160 también pueden ser redes iguales o diferentes. La red visitada 130 y la red doméstica 160 pueden o no tener un acuerdo de itinerancia. Las redes 130 y 160 pueden comprender cada una entidades que proporcionan conectividad de datos, servicios de ubicación y/u otras funcionalidades y servicios.

[18] Una red 170 puede incluir una red telefónica pública conmutada (PSTN), Internet y/u otras redes de voz y datos. Una PSTN admite la comunicación para el servicio telefónico convencional antiguo (POTS) convencional. Un PSAP 180 es una entidad responsable de responder llamadas de emergencia (por ejemplo, para servicios de policía, bomberos y médicos) y también puede denominarse Centro de Emergencia (CE). Dichas llamadas pueden iniciarse cuando el usuario marca un número fijo bien conocido, como el 911 en América del Norte o el 112 en Europa. El PSAP 180 típicamente es operado o es propiedad de una agencia gubernamental, por ejemplo, un condado o una ciudad. El PSAP 180 puede admitir la conectividad IP para llamadas de VoIP y, por lo tanto, es compatible con el protocolo de inicio de sesión (SIP), que es un protocolo de señalización para iniciar, modificar y finalizar sesiones de usuario interactivas basadas en IP, como VoIP. De forma alternativa o adicionalmente, el PSAP 180 puede admitir la comunicación con PSTN 170.

[19] Las técnicas descritas en el presente documento pueden usarse para llamadas de VoIP de emergencia originadas en redes alámbricas como DSL y cable y para llamadas de VoIP de emergencia originadas desde redes de área amplia inalámbricas (WWAN), redes de área local inalámbricas (WLAN), redes metropolitanas inalámbricas (WMAN) y redes inalámbricas con cobertura WWAN y WLAN. Las WWAN pueden ser CDMA, TDMA, FDMA, OFDMA y/u otras redes. Una red CDMA puede implementar una o más tecnologías de radio tales como CDMA de banda ancha (W-CDMA), cdma2000, etc. cdma2000 cubre las normas IS-2000, IS-856 e IS-95 e incluye revisiones Ev-DO para optimizar la admisión de IP. Una red TDMA puede implementar una o más tecnologías de radio tales como el Sistema Global para Comunicaciones Móviles (GSM), el Sistema Telefónico Móvil Digital Avanzado (D-AMPS), y así sucesivamente. D-AMPS cubre IS-248 e IS-54. W-CDMA y GSM se describen en documentos de una organización llamada "3rd Generation Partnership Project" ["Proyecto de Colaboración de Tercera Generación"] (3GPP). cdma2000 se describe en documentos de una organización llamada "3rd Generation Partnership Project 2" ["Proyecto de Colaboración de Tercera Generación 2"] (3GPP2). Los documentos del 3GPP y del 3GPP2 están a disposición del público. Una WLAN puede implementar una tecnología de radio como IEEE 802.11. Un WMAN puede implementar una tecnología de radio como IEEE 802.16. Estas diversas tecnologías y normas de radio son conocidas en la técnica.

[20] **La FIG. 2** muestra una arquitectura de red 3GPP. El UE 110 puede obtener acceso por radio a través de una red de acceso 3GPP 120a o una red de acceso WLAN 120b. La red de acceso 3GPP 120a puede ser una red de acceso por radio GSM EDGE (GERAN), una red de acceso por radio terrestre universal (UTRAN), una UTRAN evolucionada (E-UTRAN) o alguna otra red de acceso. La red de acceso 3GPP 120a incluye estaciones base 210, un subsistema de estación base (BSS)/controlador de red de radio (RNC) 212 y otras entidades no mostradas en la FIG. 2. Una estación base también se conoce como un Nodo B, un Nodo B mejorado (Nodo B), una Estación Transceptora Base (BTS), un punto de acceso (AP) o alguna otra terminología. La WLAN 120b incluye puntos de acceso 214 y puede ser cualquier WLAN.

[21] Una V-PLMN 130a es un modo de realización de la red visitada 130 en la FIG. 1 e incluye una red central V-PLMN 230a y entidades de ubicación de V-PLMN 270a. La red central V-PLMN 230a incluye un nodo de soporte GPRS de servicio (SGSN) 232a, un nodo de soporte GPRS de puerta de enlace (GGSN) 232b, una pasarela de acceso WLAN (WAG) 234 y una pasarela de datos por paquetes (PDG) 236. SGSN 232a y GGSN 232b son parte de una red central del Servicio General de Radio por Paquetes (GPRS) y proporcionan servicios de conmutación por paquetes para los UE que se comunican con la red de acceso 3GPP 120a. WAG 234 y PDG 236 son parte de una red central WLAN de interfuncionamiento de 3GPP (I-WLAN) y proporcionan servicios de conmutación por paquetes para los UE que se comunican con la WLAN 120b.

[22] La red central V-PLMN 230a también incluye un servidor de abonados locales (HSS) 250 y varias entidades de Subsistema Multimedia IP (IMS) que incluyen una Función de Control de Sesión de Llamada Proxy

(P-CSCF) 252, una CSCF de Emergencia (E-CSCF) 254, una CSCF interrogadora (I-CSCF) 256 y una función de control de pasarela de medios (MGCF) 258. P-CSCF 252, E-CSCF 254, I-CSCF 256 y MGCF 258 son compatibles con servicios IMS, por ejemplo, llamadas de VoIP, y son parte de una red V-PLMN IMS. P-CSCF 252 acepta solicitudes del UE y atiende estas solicitudes internamente o reenvía las solicitudes a otras entidades, posiblemente después de la traducción. E-CSCF 254 realiza servicios de control de sesión para los UE y mantiene el estado de sesión utilizado para admitir los servicios de emergencia del IMS. E-CSCF 254 admite, además, llamadas de VoIP de emergencia. MGCF 258 dirige la conversión de señalización entre SIP/IP y PSTN (por ejemplo, SS7 ISUP) y se utiliza siempre que una llamada de VoIP de un usuario va a un usuario de PSTN. El HSS 250 almacena información relacionada con la suscripción para los UE para los cuales V-PLMN 130a es la red doméstica.

[23] Las entidades de ubicación de V-PLMN 270a pueden incluir una plataforma de ubicación SUPL de servicios de emergencia (E-SLP) 272 y una SLP visitante (V-SLP) 274, que admiten la ubicación de plano de usuario seguro de OMA (SUPL). La V-SLP 274 puede estar dentro o estar asociada con una red diferente a la V-PLMN 130a y/o puede estar geográficamente más cerca del UE 110. De forma alternativa o adicionalmente, las entidades de ubicación de V-PLMN 270a pueden incluir un Centro de Ubicación Móvil Pasarela (GMLC) 276, que es parte de la ubicación del plano de control de 3GPP. E-SLP 272, V-SLP 274 y GMLC 276 proporcionan servicios de ubicación para los UE en comunicación con V-PLMN 130a.

[24] Una H-PLMN 160a es un modo de realización de la red doméstica 160 en la FIG. 1 e incluye una red central H-PLMN 260. La red central H-PLMN 260 incluye un HSS 266 y, además, incluye entidades IMS tales como una I-CSCF 262 y una CSCF de servicio (S-CSCF) 264 que admiten IMS para la red doméstica 160. I-CSCF 262 y S-CSCF 264 son parte de una red H-PLMN IMS.

[25] **La FIG. 3** muestra una arquitectura de red 3GPP2. El UE 110 puede obtener acceso por radio a través de una red de acceso 3GPP2 120c o una red de acceso WLAN 120d. La red de acceso 3GPP2 120c puede ser una red CDMA2000 1X, una red CDMA2000 1xEV-DO o alguna otra red de acceso. La red de acceso 3GPP2 120c incluye estaciones base 220, una Función de Control de Paquetes/Control de Recursos de Radio (RRC/PCF) 222 y otras entidades no mostradas en la FIG. 3. RRC también se puede llamar controlador de red de radio (RNC) o estación base. La red de acceso 3GPP2 120c también se puede llamar red de acceso por radio (RAN). La WLAN 120d incluye puntos de acceso 224 y puede ser cualquier WLAN asociada con una red 3GPP2.

[26] Una V-PLMN 130b es otro modo de realización de la red visitada 130 en la FIG. 1 e incluye una red central V-PLMN 230b y entidades de ubicación 3GPP2 270b. La red central V-PLMN 230b incluye un Nodo de Servicio de Datos por Paquetes (PDSN) 242, una Función de Interfuncionamiento de Datos por Paquetes (PDIF) 244 y un servidor de Autenticación, Autorización y Contabilidad (AAA) 246. PDSN 242 y PDIF 244 proporcionan servicios de conmutación de paquetes para los UE que se comunican con la red de acceso 3GPP2 120c y WLAN 120d, respectivamente. La red central V-PLMN 230a también incluye entidades IMS o de dominio multimedia (MMD) tales como P-CSCF 252, E-CSCF 254, I-CSCF 256 y MGCF 258. E-CSCF 258 también puede tener otros nombres, como ES-AM (Administrador de aplicaciones de servicios de emergencia).

[27] Las entidades de ubicación 3GPP2 270b pueden incluir E-SLP 272 y V-SLP 274 para SUPL. De forma alternativa o adicionalmente, las entidades de ubicación 3GPP2 270b pueden incluir un Servidor de Posición de Servicios de Emergencia (E-PS) 282 y un Servidor de Posición Visitada (V-PS)/Entidad Determinante de Posición (PDE) 284, que son parte de la ubicación X.S0024 para redes cdma2000. E-PS 282 también puede denominarse servidor de posición sustituto (S-PS). E-SLP 272, V-SLP 274, E-PS 282 y V-PS/PDE 284 proporcionan servicios de ubicación para los UE en comunicación con V-PLMN 130b.

[28] Para simplificar, las FIGs. 2 y 3 muestran solo algunas de las entidades en 3GPP y 3GPP2, que se mencionan en la descripción a continuación. Las redes 3GPP y 3GPP2 pueden incluir otras entidades definidas por 3GPP y 3GPP2, respectivamente.

[29] En la siguiente descripción, las redes 3GPP se refieren a redes y subsistemas de red (por ejemplo, subsistemas de red de acceso) definidos por 3GPP así como a otras redes y subsistemas de red (por ejemplo, WLAN) que funcionan conjuntamente con redes 3GPP. Las redes 3GPP y los subsistemas de red pueden incluir GERAN, UTRAN, E-UTRAN, red central GPRS, red IMS, I-WLAN 3GPP y más. Las redes 3GPP2 se refieren a redes y subsistemas de red definidos por 3GPP2, así como a otras redes y subsistemas de red que funcionan conjuntamente con redes 3GPP2. Las redes 3GPP2 pueden incluir CDMA2000 1X, CDMA2000 1xEV-DO, red central cdma2000, subsistema de red 3GPP2 IMS o MMD, WLAN asociada 3GPP2 y más. Para simplificar, "WLAN 3GPP" se refiere a una WLAN asociada con una red 3GPP, y "WLAN 3GPP2" se refiere a una WLAN asociada con una red 3GPP2.

[30] En la siguiente descripción, el acceso GPRS se refiere al acceso a la red central GPRS a través de GERAN, UTRAN o alguna otra red de acceso 3GPP. El acceso WLAN 3GPP se refiere al acceso a la red central 3GPP a través de una WLAN. El acceso cdma2000 se refiere al acceso a la red central de cdma2000 a través de

CDMA2000 1X, CDMA2000 1xEV-DO o alguna otra red de acceso 3GPP2. El acceso WLAN 3GPP2 se refiere al acceso a la red central WLAN 3GPP2 a través de una WLAN.

[31] Para 3GPP, el UE 110 puede o no estar equipado con una Tarjeta de Circuito Integrado Universal (UICC). Para 3GPP2, el UE 110 puede o no estar equipado con un Módulo de Identidad de Usuario (UIM). Una UICC o un UIM es típicamente específico para un suscriptor y puede almacenar información personal, información de suscripción y/u otra información. Un UE sin UICC es un UE sin una UICC, y un UE sin UIM es un UE sin un UIM. Un UE sin UICC/UIM no tiene suscripción, ni red doméstica ni credenciales de autenticación (por ejemplo, ninguna clave secreta) para verificar cualquier identidad reclamada, lo que hace que los servicios de ubicación sean más propensos a los riesgos.

[32] Las técnicas descritas en el presente documento se pueden usar para diversas arquitecturas de ubicación tales como las arquitecturas de plano de control y de plano de usuario. Un plano de control (que también se llama plano de señalización) es un mecanismo para llevar la señalización para aplicaciones de capa superior y se implementa típicamente con protocolos, interfaces y mensajes de señalización específicos de la red. Un plano de usuario es un mecanismo para transferir señalización para aplicaciones de capa superior, pero empleando una portadora de plano de usuario, que se implementa típicamente con protocolos tales como el protocolo de datagramas de usuario (UDP), el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP), todos los cuales son bien conocidos en la técnica. Los mensajes de admisión de servicios de ubicación y posicionamiento se llevan como parte de la señalización en una arquitectura de plano de control y como parte de datos (desde una perspectiva de red) en una arquitectura de plano de usuario. Sin embargo, el contenido de los mensajes puede ser el mismo o similar en ambas arquitecturas.

[33] Las técnicas se pueden usar para diversas arquitecturas/soluciones de ubicación tales como las enumeradas en la Tabla 1. SUPL y pre-SUPL se describen en documentos de la Alianza Móvil Abierta (OMA). El plano de control 3GPP se describe en TS 23.271, TS 43.059 y TS 25.305 de 3GPP. El plano de control 3GPP2 se describe en IS-881 y X.S0002 de 3GPP2. El plano de usuario 3GPP2 se describe en X.S0024 de 3GPP2.

Tabla 1

Arquitectura de ubicación	Tipo de arquitectura	Aplicable para ...
Pre-SUPL	plano de usuario	redes 3GPP
SUPL	plano de usuario	redes 3GPP y 3GPP2
plano de control 3GPP	plano de control	redes 3GPP
plano de control 3GPP2	plano de control	redes 3GPP2
X.S0024	plano de usuario	redes 3GPP2

[34] Un UE puede admitir cero, una o múltiples soluciones de ubicación (por ejemplo, SUPL o plano de control 3GPP o SUPL y plano de control 3GPP, o SUPL y X.S0024) para llamadas de VoIP de emergencia. El UE puede informar a la red de sus capacidades de ubicación cuando se realiza una llamada, por ejemplo, en un mensaje SIP INVITAR y/o SIP REGISTRAR. Esta información puede almacenarse en un servidor local (por ejemplo, un servidor de ubicación) para su recuperación por la red.

[35] Las técnicas descritas en el presente documento pueden admitir las siguientes características.

(a) Admite llamadas de VoIP de emergencia para usuarios móviles, fijos y nómadas.

(b) Aplicable a llamadas de VoIP usando acceso GPRS, acceso WLAN 3GPP, acceso cdma2000 y acceso WLAN 3GPP2.

(c) Admite la conectividad IP de extremo a extremo para PSAP compatibles con SIP/IP.

(d) Admite la conectividad a PSAP compatibles con PSTN, que pueden ser locales para los UE que llaman pero geográficamente alejados de los servidores de llamadas SIP, por ejemplo, cuando un proveedor de servicios de VoIP está alejado de un UE.

(e) Admite el encaminamiento de llamadas a un PSAP adecuado utilizando una estimación de posición provisional.

(f) Proporciona ubicación precisa del UE al PSAP.

(g) Admite ubicación inicial y actualizada usando varias arquitecturas de ubicación.

(h) Admite llamadas de VoIP de emergencia desde UE sin UICC/UIM y UE cuyas H-PLMN no tienen acuerdos de itinerancia con V-PLMN.

(i) Admite la devolución de llamada desde un PSAP a un UE sin UICC/UIM y/o sin acuerdo de itinerancia en una V-PLMN.

(j) Compatible con una solución IETF Ecrit y soluciones NENA como la arquitectura de VoIP provisional para los servicios 9-1-1 mejorados (i2), también conocida como solución NENA I2.

(k) Pequeños impactos y requisitos para H-PLMN.

[36] La devolución de llamada del PSAP se refiere a una llamada de un PSAP a un UE, por ejemplo, debido a que la llamada de emergencia se interrumpió o se liberó demasiado pronto. Una estimación de posición provisional típicamente se refiere a una posición aproximada utilizada para el encaminamiento, y una estimación de posición inicial típicamente se refiere a la primera estimación precisa de posición. En algunos casos, la estimación de la posición inicial puede obtenerse después de la estimación de la posición provisional. En otros casos, las estimaciones de posición provisional e inicial pueden ser las mismas. En algunos otros casos, la estimación de la posición provisional y/o la estimación de la posición inicial no se pueden utilizar.

[37] Para SUPL, una SLP doméstica (H-SLP) en H-PLMN 160 puede ignorarse, y se pueden usar una o más V-SLP y/o E-SLP en o asociados con V-PLMN 130 para la ubicación. Para X.S0024, un PS doméstico (H-PS) en H-PLMN 160 puede ignorarse, y pueden usarse uno o más V-PS y/o E-PS en o asociados con V-PLMN 130 para su ubicación. Esto implica algunos cambios en SUPL y X.S0024, por ejemplo, la H-SLP o el H-PS configurados en el UE 110 pueden anularse para la ubicación durante una llamada de emergencia. El uso de V-SLP(s), E-SLP, E-PS o V-PS(s) en V-PLMN 130 puede ser conveniente por las siguientes razones:

(a) La admisión de llamadas de emergencia especializada en regiones o países específicos debe contar con el apoyo de solo redes en esas regiones y no otras redes.

(b) Un UE sin UICC/UIM puede no tener H-PLMN y puede depender de una SLP o un PS en la V-PLMN.

(c) Para un UE con UICC/UIM, la H-PLMN puede no tener acuerdos de itinerancia con la V-PLMN, y puede ser difícil usar la H-SLP o el H-PS.

(d) La H-SLP o el H-PS puede no admitir una solicitud de ubicación de un PSAP remoto (por ejemplo, en otro país) debido a diferencias de señalización y falta de registro.

(e) La H-SLP o el H-PS pueden no ser capaces de obtener una buena estimación de posición (por ejemplo, si la H-SLP o el H-PS está alejado del UE) sin la asistencia de una V-SLP o un V-PS en la V-PLMN.

(f) La H-SLP o el H-PS pueden no admitir una interfaz (por ejemplo, una interfaz Li o LCS-i) utilizada por la E-SLP o el E-PS para admitir servicios de llamadas de emergencia.

[38] E-SLP 272 o E-PS 282 pueden realizar el posicionamiento para el UE 110 en SUPL y X.S0024, respectivamente. De forma alternativa, se puede seleccionar una V-SLP, un V-PS o una PDE para realizar el posicionamiento para el UE 110, por ejemplo, si E-SLP 272 o E-PS 282 no pueden realizar esta función. Una V-SLP, un V-PS o una PDE puede ser útil, por ejemplo, si un servidor de llamadas SIP (por ejemplo, E-CSCF 254) está alejado del UE 110 y selecciona una E-SLP o un E-PS que también es remoto, que puede ocurrir cuando un operador usa una pequeña cantidad de servidores de llamadas para dar servicio a una región grande o a todo un país. E-SLP 272 o E-PS 282 pueden seleccionar una V-SLP, un V-PS o una PDE apropiados usando cualquiera de los siguientes mecanismos:

(a) El UE 110 descubre una dirección IP o nombre de una V-SLP o un V-PS cuando se conecta a una red de acceso o establece una conectividad IP, por ejemplo, la red de acceso proporciona la dirección V-SLP o V-PS al UE 110. El UE 110 también puede descubrir la dirección V-SLP o V-PS mediante una consulta DNS después de establecer la conectividad IP. Esto puede ser aplicable si un servidor DNS utilizado por el UE 110 es más local para el UE 110 que la E-CSCF 254. El UE 110 puede incluir la dirección V-SLP o V-PS en un SIP REGISTRAR inicial enviado al IMS y en cualquier otro REGISTRO subsiguiente después del traspaso a una nueva red de acceso. IMS (por ejemplo, E-CSCF 254) puede transferir la dirección V-SLP o V-PS a E-SLP 272 o E-PS 282.

(b) E-SLP 272 o E-PS 282 determina la dirección V-SLP o V-PS en base a la información de ubicación proporcionada por el UE 110 en el SIP INVITAR inicial.

(c) E-SLP 272 o E-PS 282 determina la dirección V-SLP o V-PS en base a la información de ubicación recibida desde el UE 110 en un SUPL INICIO.

[39] En general, la información de ubicación proporcionada por el UE 110 puede ser cualquier información que pueda usarse para determinar la posición del UE 110. La información de ubicación puede comprender coordenadas geográficas, GSM, UMTS o identidad de célula cdma2000 (ID), información de la célula de servicio cdma2000, identidad de nombre de acceso WLAN, dirección MAC de WLAN, etc. La información de ubicación también puede comprender mediciones que pueden usarse para determinar la posición del UE 110.

[40] Para SUPL y X.S0024, E-SLP 272 o E-PS 282 pueden enviar un SUPL INIT al UE 110 para iniciar una sesión SUPL. El SUPL INIT puede enviarse mediante un WAP Push o SMS, lo que puede ocasionar un retardo mayor. En un modo de realización, para reducir el retardo, el SUPL INIT puede enviarse al UE 110 a través del IMS (por ejemplo, P-CSCF 252 y E-CSCF 254) usando un mensaje IMS inmediato, algún otro mensaje IMS, una respuesta SIP 1xx (por ejemplo, un progreso de la sesión 183) o algún otro mensaje. El uso de asociaciones existentes (posiblemente seguras) entre el IMS y el UE 110 permite una transferencia rápida y además evita un retardo adicional para establecer nuevas asociaciones y/o transferir el mensaje a través de entidades adicionales (por ejemplo, un centro de servicio de SMS). Este modo de realización también se puede usar cuando el UE 110 no está registrado en la H-PLMN, por ejemplo, no tiene UICC o UIM. En otro modo de realización, para reducir el retardo, el SUPL INIT puede enviarse al UE 110 usando una IP con terminación móvil o UDP/IP. En este caso, una pasarela IP que sirve al UE 110 (por ejemplo, GGSN 232b, PDG 236, PDSN 242 o PDIF 244) puede ser preadministrada con la dirección o direcciones IP de E-SLP 272 para no filtrar los paquetes IP de E-SLP 272 al UE 110. El UE 110 se puede configurar para admitir un puerto TCP y/o un puerto UDP usado para SUPL (y registrado con IANA) para recibir el SUPL INIT.

[41] Las llamadas de VoIP de emergencia pueden ser compatibles con SUPL 1.0 y la versión inicial de X.S0024 (X.S0024-0 de 3GPP2) de la siguiente manera.

(a) Si el UE 110 está en H-PLMN 160, entonces el E-SLP 272 es el H-SLP o el E-PS 282 es el H-PS para el UE e invoca una solicitud de ubicación iniciada por la red SUPL 1.0 o X.S0024-0. Un SUPL INIT puede enviarse al UE 110 usando SMS o WAP Push.

(b) Si el UE 110 no está en H-PLMN 160 pero está registrado en V-PLMN 130, entonces E-SLP 272 puede invocar una solicitud de ubicación SUPL 1.0 actuando como una SLP Solicitante (R-SLP) y enviando la solicitud de ubicación a la H-SLP para el UE 110 de acuerdo con el procedimiento en SUPL 1.0 y OMA RLP. De forma similar, el E-PS 282 puede invocar una solicitud de ubicación X.S0024 desde el H-PS para el UE 110 usando, por ejemplo, el protocolo OMA RLP.

(c) Si el UE 110 no está en H-PLMN 160 y no está registrado en V-PLMN 130 (por ejemplo, no hay acuerdo de itinerancia entre V-PLMN 130 y H-PLMN 160) o si el UE 110 no tiene UICC o UIM, entonces no admite la ubicación SUPL 1.0 o X.S0024-0. Sin embargo, E-SLP 272 o E-PS 282 todavía pueden ser capaces de obtener una estimación de posición para el UE 110 usando información de ubicación proporcionada por el UE 110 en un SIP INVITAR inicial para una llamada de emergencia.

1. Llamada de VoIP de emergencia con SUPL

[42] **La FIG. 4** muestra un diagrama de bloques de un modo de realización de una arquitectura de red 400 para llamadas de VoIP de emergencia con ubicación SUPL. La arquitectura de red 400 es aplicable tanto para redes 3GPP como 3GPP2. Para simplificar, la FIG. 4 muestra solo las entidades e interfaces relevantes para admitir llamadas de VoIP de emergencia usando SUPL.

[43] El UE 110 se denomina terminal habilitado para SUPL (SET) en SUPL. La red de acceso 120 puede ser una red de acceso 3GPP, una red de acceso 3GPP2, una WLAN o alguna otra red. La red de acceso 120 y/o la V-PLMN 130 incluyen entidades que admiten llamadas de conmutación por paquetes, por ejemplo, como se muestra en las FIGs. 2 y 3. Para 3GPP2, IP simple y/o IP móvil pueden usarse para llamadas de VoIP de emergencia. En la siguiente descripción, IMS puede referirse a P-CSCF 252, E-CSCF 254 y/o MGCF 258.

[44] La E-SLP 272 puede incluir un Centro de Ubicación SUPL (E-SLC) 412 que realiza varias funciones para los servicios de ubicación y un Centro de Posicionamiento SUPL (E-SPC) 414 que admite el posicionamiento para los UE. V-SLP 274 puede incluir de manera similar un V-SLC 422 y un V-SPC 424. E-SLP 272 puede sustituir a una H-SLP en H-PLMN 160 en caso de ubicación para llamadas de emergencia. Las entidades en SUPL se describen en un documento OMA-AD-SUPL-V2_0-20060704-D, titulado "Secure User Plane Location Architecture" ["Arquitectura de ubicación segura de plano de usuario"], versión preliminar 4.0, 4 de julio de 2006 y en el documento OMA-TS-ULP-V2_0- 20060721-D, titulado "User Plane Location Protocol" ["Protocolo de ubicación del plano de usuario"], versión preliminar 2.0, 21 de julio de 2006, que está disponible para el público en OMA.

[45] SUPL admite dos modos de comunicación entre un SET y una SLP para el posicionamiento con un SPC. En un modo proxy, el SPC no tiene comunicación directa con el SET, y la SLP actúa como un proxy entre el SET y el SPC. En un modo no proxy, el SPC tiene comunicación directa con el SET.

[46] PSTN/Internet 170 puede incluir entidades (por ejemplo, encaminadores) que admiten encaminamiento de paquetes y un encaminador selectivo (S/R) 292 que encamina una llamada de emergencia a un PSAP. S/R 292 puede pertenecer a PSAP 180 o puede ser compartido por y conectado a un conjunto de PSAP individuales. El UE 110 puede comunicarse con PSAP 180 a través de P-CSCF 252 y E-CSCF 254 para una llamada de VoIP si PSAP 180 admite SIP. El UE 110 también puede comunicarse con PSAP 180 a través de P-CSCF 252, E-CSCF 254, MGCF 258 y S/R 292 si PSAP 180 no admite SIP. En este caso, una pasarela de medios (MGW) controlada por MGCF 258 realiza conversión de modo de circuito de VoIP a PCM para la llamada de emergencia.

[47] La FIG. 4 también muestra las interfaces entre varias entidades. Las interfaces relacionadas con la llamada entre el UE 110, P-CSCF 252, E-CSCF 254, MGCF 258 pueden ser SIP. Las interfaces relacionadas con la llamada entre MGCF 258, S/R 292 y PSAP 180 pueden ser MF/ISUP. La interfaz relacionada con la ubicación entre PSAP 180 y E-SLP 272 puede ser una interfaz E2 definida en J-STD-036 revisión B si PSAP 180 admite PSTN o una extensión de la interfaz E2 si el PSAP 180 admite SIP. La interfaz relacionada con la ubicación entre PSAP 180 y E-SLP 272 puede ser en su lugar una interfaz MLP definida en OMA o protocolo de ubicación móvil LIF o en alguna otra interfaz, por ejemplo, una interfaz HTTP. La interfaz relacionada con la ubicación entre el UE 110 y V-SLP 274 y E-SLP 272 puede ser SUPL ULP.

[48] Se usa una interfaz entre E-CSCF 254 y E-SLP 272 para transmitir información sobre el UE 110 a E-SLP 272 y para instigar el posicionamiento SUPL. Esta interfaz puede ser una interfaz LCS IMS (por ejemplo, Li) y puede utilizar un protocolo de ubicación IMS (ILP) o algún otro protocolo. La interfaz Li/ILP puede ser similar a una interfaz de protocolo de ubicación itinerante OMA (RLP) entre las SLP. La interfaz Li/ILP puede ser utilizada por cualquier entidad IMS (por ejemplo, una S-CSCF o Servidor de aplicaciones) y E-SLP 272 para admitir otras características asociadas con IMS y servicios basados en IP tales como:

(a) Facturación dependiente de la ubicación para VoIP u otras llamadas basadas en IP,

(b) Suministro de la ubicación de una de las partes de una llamada a una o más partes, y

(c) Servicios suplementarios basándose en la ubicación del usuario, por ejemplo, desvío de llamadas dependiente de la ubicación, restricción de llamadas dependiente de la ubicación.

[49] La interfaz entre E-SLP 272 y E-CSCF 254 también puede ser una interfaz v2 definida en "Draft NENA Standards for VoIP/Packet Migration i2 Solutions" ["Borradores Normas NENA para Soluciones i2 VoIP/Migración de paquetes"] o en "Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)" ["Arquitectura VoIP provisional para servicios 9-1-1 mejorados (i2)"] (en lo sucesivo, la "solución NENA I2"), que se está considerando para la admisión de VoIP E911 en los Estados Unidos, o en alguna otra interfaz.

[50] La arquitectura de red 400 puede incluir otras entidades para admitir VoIP y/o ubicación, por ejemplo, los elementos descritos en la solución NENA I2 o el borrador de las soluciones NENA I2.5 e I3.

1.1. <u>Configuración de llamada</u>

[51] **La FIG. 5** muestra un modo de realización de un flujo de mensajes 500 para la configuración de llamadas de VoIP de emergencia usando SUPL. Para mayor claridad, las entidades que son menos relevantes (por ejemplo, la red de acceso 120, P-CSCF 252, S/R 292) se omiten en la FIG. 5 pero están incluidas en las descripciones a continuación. El flujo de mensajes 500 se puede usar para redes 3GPP y 3GPP2. El flujo de mensajes 500 supone que el UE 110 tiene una UICC o un UIM y que existe un acuerdo de itinerancia entre H-PLMN 160 y V-PLMN 130.

[52] En la etapa 1, el UE 110 descubre una red de acceso (AN), por ejemplo, una red de acceso 3GPP, una red de acceso 3GPP2, una WLAN 802.11, etc. El UE 110 realiza cualquier conexión de bajo nivel (por ejemplo, asociación 802.11) y se conecta a la red de acceso (por ejemplo, a través de conexión GPRS o procedimiento WLAN AAA para 3GPP). El UE 110 establece conectividad IP y puede descubrir una dirección de servidor SIP local. En la descripción a continuación, P-CSCF 252 es el servidor SIP local descubierto por el UE 110. La etapa 1 se puede realizar de diferentes maneras para diferentes redes y se describe con más detalle a continuación.

[53] En la etapa 2, el UE 110 envía un SIP REGISTRAR a P-CSCF 252, que es el servidor SIP local descubierto en la etapa 1. El SIP REGISTRAR puede incluir una indicación de servicios de emergencia, un ID de usuario público de emergencia (por ejemplo, como se describe en TR 23.867 de 3GPP y en TS 23.167 de 3GPP), un ID de usuario privado, un nombre de dominio H-PLMN y una dirección IP del UE obtenida en la etapa 1. El SIP REGISTRAR también puede incluir información de ubicación para el UE 110, las capacidades de ubicación del UE 110, y/u otra información. Las capacidades de ubicación del UE pueden comprender las

soluciones de ubicación admitidas por el UE 110 (por ejemplo, SUPL, plano de control 3GPP, X.S0024, etc.), los procedimientos de posicionamiento admitidos por el UE 110, y/u otra información. Debido a la presencia de la indicación de servicios de emergencia o al ID de usuario público de emergencia, P-CSCF 252 envía el SIP REGISTRAR a E-CSCF 254 en la misma red, y no a I-CSCF 262 en H-PLMN 160 como en casos que no sean de emergencia.

[54] En la etapa 3, E-CSCF 254 en V-PLMN 130 envía el SIP REGISTRAR a S-CSCF 264 en H-PLMN 160 donde se produce el registro IMS normal. Las razones para registrarse en H-PLMN 160 son (1) para autenticar la identidad del usuario, (2) para obtener un número de devolución de llamada verificado de S-CSCF 264, (3) para alertar a H-PLMN 160 de la llamada de emergencia para que se aplique un tratamiento especial (por ejemplo, prioridad, restricción de servicios suplementarios) si PSAP 180 llama más tarde al UE 110 a través de H-PLMN 160. Para el registro del IMS, S-CSCF 264 en H-PLMN 160 trata a E-CSCF 254 en V-PLMN 130 como una P-CSCF. Un URI del TEL de usuario público (por ejemplo, obtenido de un MSISDN en 3GPP o un MIN en 3GPP2) puede registrarse implícitamente con el ID de usuario público de emergencia para el UE 110 y puede usarse para la devolución de llamada de PSAP desde una PSTN. H-PLMN 160 puede no admitir el registro adicional del ID de usuario público de emergencia, por ejemplo, si el UE 110 ya había registrado un ID de usuario público normal o si el ID de usuario público de emergencia no es compatible con H-PLMN 160. E-CSCF 254 puede mantener una lista de H-PLMN para las cuales se puede saltar la etapa 3. Si se omite la etapa 3, la devolución de la llamada desde el PSAP 180 aún puede ser posible usando un ID de usuario público normal del UE 110, que debe ser registrado por el UE 110 por separado. El E-CSCF 254 también puede asignar un ID de usuario público temporal al UE 110, como se describe a continuación, para habilitar la devolución de llamada desde el PSAP 180 directamente a través de V-PLMN 130 y no a través de H-PLMN 160. Este ID de usuario público temporal puede ser especialmente útil para un UE itinerante extranjero ya que se pueden mejorar tanto el retardo como la fiabilidad de la devolución de llamada. Si el registro en H-PLMN 160 no se realiza, entonces el UE 110 no se autentica y no se puede establecer una conexión IP segura entre el UE 110 y E-CSCF 254 en la V-PLMN 130, lo que puede degradar la seguridad para la ubicación posterior del UE 110 por E-SLP 272.

[55] En la etapa 4, E-CSCF 254 (por ejemplo, después de recibir un SIP 200 OK de H-PLMN 160) devuelve un 200 OK al UE 110. Después de la configuración de la llamada de emergencia, si el UE 110 se transfiere dentro de la misma V-PLMN a un SGSN diferente (para acceso GPRS), una WLAN diferente (para acceso WLAN), o una PCF o PDSN diferente (para acceso cdma2000), luego, el UE 110 puede volverse a registrar repitiendo las etapas 2 a 4 a fin de actualizar la información de ubicación y V-SLP. Si el UE 110 vuelve a registrarse usando su ID de usuario público de emergencia, entonces E-CSCF 254 puede transferir cualquier nueva información de ubicación a E-SLP 272. El nuevo registro permite que se elija una V-SLP diferente si el UE 110 se ha movido fuera del área geográfica admitida por la V-SLP anterior.

[56] Para el acceso WLAN 3GPP2, se puede realizar un procedimiento de transferencia si el UE 110 se mueve de una WLAN a otra WLAN o de una WLAN a una red cdma2000. El procedimiento de transferencia puede establecer un nuevo túnel al PIDF anterior desde la nueva WLAN (para el traspaso de una WLAN a otra WLAN) o desde la nueva PDSN (para el traspaso desde una WLAN a una red cdma2000) para continuar usando la dirección IP asociada con la PDIF anterior y para evitar la interrupción de la llamada de VoIP de emergencia. Para el traspaso de una red cdma2000 a una WLAN, la PDIF asociada con la nueva WLAN puede emular una PDSN objetivo para admitir el traspaso rápido a la PDSN de servicio previa. Después del traspaso, el UE 110 puede volver a registrarse para proporcionar a E-CSCF 254 nueva información de ubicación relevante para la selección de V-SLP.

[57] En un modo de realización alternativo de las etapas 2, 3 y 4, después de que el UE 110 envíe un SIP REGISTRAR a P-CSCF 252 en la etapa 2, P-CSCF 252 puede reenviar el SIP REGISTRAR directamente a S-CSCF 264 en H-PLMN 160 o a I-CSCF 262 en H-PLMN 160 y omita E-CSCF 254 en V-PLMN 130. En este caso, un SIP 200 OK de H-PLMN 160 se devolvería a P-CSCF 252 en lugar de a E-CSCF 254, y P-CSCF 252 devolvería el 200 OK al UE 110 en la etapa 4. Este modo de realización alternativo puede reducir o evitar impactos especiales a P-CSCF 252 para admitir llamadas de emergencia de VoIP porque las acciones P-CSCF 252 son entonces similares a las del registro normal.

[58] En la etapa 5, el UE 110 envía un SIP INVITAR a P-CSCF 252. El SIP INVITAR puede incluir un URL de SIP o URI del TEL global que indique una llamada de emergencia (por ejemplo, sos@dominio-local o "911" propuesto por IETF Ecrit) y el tipo de servicio de emergencia solicitado. El SIP INVITAR también puede incluir información relativa a la ubicación del UE que está disponible para el UE 110 (por ejemplo, una ID de célula cdma2000 o GPRS, una dirección MAC WLAN AP, etc.), capacidades de ubicación del UE 110 si no se proporciona durante el registro, información de contacto para la devolución de llamada, y/u otra información. La información de devolución de llamada puede incluir un URI del TEL (por ejemplo, derivado del MSISDN de 3GPP o MDN de 3GPP2) y posiblemente un URL de SIP (por ejemplo, el ID de usuario público de emergencia utilizado en la etapa 2). Un campo de cabecera "admitido" del SIP REGISTRAR o SIP INVITAR también se puede usar para transmitir las capacidades de ubicación del UE. Las capacidades de ubicación también se pueden incluir como parte de la información de ubicación proporcionada por el UE (por ejemplo en el objeto IETF Geopriv pidf-lo) o de alguna otra manera en el SIP INVITAR. P-CSCF 252 puede reenviar SIP INVITAR a otro servidor SIP,

que puede reenviar el SIP INVITAR a un proxy de encaminamiento (por ejemplo, un Servidor de Aplicaciones) dedicado a llamadas de emergencia. En la FIG. 5, E-CSCF 254 es el servidor SIP que maneja las llamadas de emergencia.

[59] En la etapa 6, la E-CSCF 254 puede determinar explícita o implícitamente que el UE 110 admite SUPL y envía una solicitud de encaminamiento (o una solicitud de ubicación de emergencia) a la E-SLP 272. La solicitud de encaminamiento puede incluir las identidades públicas del UE (por ejemplo, el ID de usuario público de emergencia de la etapa 5, el URI del TEL, etc.), cualquier información de ubicación recibida por E-CSCF 254 y la dirección IP del UE si en la etapa 8 se usará IP con terminación móvil (o UDP/IP). E-SLP 272 puede estar en la misma red que E-CSCF 254 o en alguna otra red. E-SLP 272 se puede seleccionar porque cubre un área geográfica que incluye una ubicación aproximada del UE 110. E-CSCF 254 puede seleccionar E-SLP 272, un servidor genérico de ubicación capaz de actuar como una E-SLP, o algunos otros tipos de servidor, por ejemplo, GMLC 276. El servidor de ubicación seleccionado puede elegir usar SUPL basándose en las capacidades de ubicación del UE transferidas por E-CSCF 254 (o simplemente por suposición). El E-CSCF 254 puede solicitar información de ubicación de la E-SLP 272 y/o la selección de un PSAP correspondiente a la información de ubicación disponible y al tipo de servicio de emergencia.

[60] E-SLP 272 avanza a la etapa 12 si la información de ubicación proporcionada en la etapa 6 permite a E-SLP 272 obtener una estimación de posición para el UE 110 que es lo suficientemente precisa para cumplir la solicitud en la etapa 6 (por ejemplo, determinar un PSAP de destino únicamente). De lo contrario, las etapas 7 a 11 se realizan para obtener una estimación de posición adecuada para el UE 110.

[61] En la etapa 7, la E-SLP 272 determina a partir de la información de ubicación recibida si usar una V-SLP por separado para ayudar con la ubicación. Si es así, entonces se puede seleccionar una V-SLP (por ejemplo, V-SLP 274) basándose en la información de ubicación recibida de E-CSCF 254. E-SLP 272 actúa como H-SLP en la realización de la ubicación SUPL posterior usando procedimientos que pueden ser similares a los utilizados para (a) admitir itinerancia SUPL 1.0 si se seleccionó una V-SLP o (b) no admitir itinerancia SUPL 1.0 si una V-SLP no fue seleccionada. En el caso de itinerancia, E-SLP 272 puede intercambiar alguna señalización RLP preliminar con V-SLC 422, que no se muestra en la FIG. 5. La E-SLP 272 luego genera un SUPL INIT para instigar un procedimiento de ubicación iniciado en la red con el UE 110 usando modos proxy o no proxy en SUPL. La E-SLP 272 puede enviar el SUPL INIT directamente al UE 110 usando un IP con terminación móvil o UDP/IP, en cuyo caso se puede omitir la etapa 8. E-SLP 272 también puede enviar el SUPL INIT dentro de un mensaje inmediato (por ejemplo, un mensaje IMS inmediato o algún otro mensaje IMS o SIP) a E-CSCF 254. En cualquier caso, el SUPL INIT puede incluir una dirección IP de un SPC utilizado para posicionamiento (que puede ser E-SPC 414 o V-SPC 424 si no se usa el modo proxy), requisitos de precisión/retardo de calidad de posición (QoP) para una estimación de posición provisional rápida, una indicación de modo proxy/no proxy, datos de autenticación y/u otra información. El SUPL INIT también puede incluir una dirección IP de E-SLP 272, por ejemplo, si el UE 110 no está en su red doméstica, si E-SLP 272 no es la H-SLP para el UE 110, o si E-SLP 272 es la H-SLP, pero elige no comportarse como H-SLP (por ejemplo, para evitar admitir más de un procedimiento para llamadas de emergencia). El SUPL INIT también puede incluir una indicación de llamada de emergencia, por ejemplo, en un parámetro de notificación SUPL INIT.

[62] En la etapa 8, E-CSCF 254 envía el SUPL INIT al UE 110 a través de P-CSCF 252 usando un mensaje IMS inmediato, algún otro mensaje IMS, una respuesta SIP 1xx (por ejemplo, un progreso de sesión 183), o alguna otro mensaje basado en IP que usa asociaciones de IP seguras entre E-CSCF 254, P-CSCF 252 y UE 110 establecidas en las etapas 2 a 4.

[63] En la etapa 9, el UE 110 establece una conexión de IP segura (por ejemplo, TCP/IP seguro) a E-SLP 272, que puede ser H-SLP para el UE 110 o puede haber incluido su dirección en el SUPL INIT enviado en la etapa 7. Para el modo no proxy, el UE 110 obtiene datos de autenticación de la E-SLP 272 (no mostrado) y establece una conexión segura de IP a E-SPC 414 o V-SPC 424 con autenticación mutua. El E-SLC 412 también transmite información a E-SPC 414 o V-SPC 424 para el modo no proxy (no mostrado en la FIG. 5). El UE 110 puede obtener mediciones relacionadas con la ubicación (por ejemplo, niveles de señal y/o temporización de células vecinas) o una estimación de posición (por ejemplo, usando un GPS independiente) coherente con la QoP recibida. El UE 110 luego devuelve un POS INIT SUPL a E-SLP 272 (para el modo proxy) o E-SPC 414 o V-SPC 424 (para el modo no proxy, que no se muestra en la FIG. 5). POS INIT SUPL puede incluir un código hash utilizado para la autenticación en modo proxy, las capacidades de posicionamiento del UE, una estimación de posición o una solicitud de datos de asistencia A-GPS (que también pueden incluirse en un mensaje POS SUPL integrado para IS-801). El POS INIT SUPL también puede incluir mediciones relacionadas con la ubicación para ayudar a obtener una estimación rápida de la posición provisional y evitar más señalización POS SUPL. Para 3GPP, las mediciones pueden comprender niveles de señal de estaciones base o puntos de acceso vecinos, avance temporal de GPRS, diferencia temporal WCDMA Rx-Tx, etc. Para 3GPP2, las mediciones pueden comprender mediciones relacionadas con la ubicación relevantes para cdma2000 o WLAN 3GPP2.

[64] En la etapa 10, E-SLP 272, E-SPC 414 o V-SPC 424 pueden intercambiar mensajes de POS SUPL adicionales con el UE 110 si no se recibió una estimación de posición adecuada (o mediciones de ubicación) en

la etapa 9. Cada mensaje POS SUPL puede incluir un mensaje de posicionamiento RRLP, RRC o IS-801 integrado. Este intercambio de mensajes continúa hasta que se proporcionen medidas de posicionamiento adecuadas o una estimación de posición para E-SLP 272, E-SPC 414 o V-SPC 424. En la etapa 11, se devuelve un SUPL FIN al UE 110 para cerrar la transacción SUPL.

[65] En la etapa 12, E-SLP 272, E-SPC 414 o V-SPC 424 calcula una estimación de posición provisional para el UE 110 a partir de la información de ubicación recibida en la etapa 9 o en la etapa 10. Para el modo no proxy, E-SPC 414 o V-SPC 424 transmite la estimación de la posición a E-SLC 412. Basándose en la estimación de la posición, y si lo solicita E-CSCF 254 en la etapa 6, E-SLP 272 selecciona un PSAP. La siguiente descripción supone que el PSAP 180 es el PSAP seleccionado. Si el PSAP 180 tiene acceso/capacidad PSTN, entonces E-SLP 272 obtiene (a) un número de directorio no marcable de dígitos de encaminamiento de servicios de emergencia (ESRD) que puede usarse para encaminar al PSAP 180 y (b) un número de directorio no marcable de clave de encaminamiento de servicios de emergencia (ESRK) que identifica PSAP 180, E-SLP 272 y, temporalmente, el UE 110. Cada PSAP puede estar asociado con un ESRD así como con un grupo de ESRK que identifique a E-SLP 272 y ese PSAP. Para cada llamada de emergencia de un UE a este PSAP, un ESRK del grupo puede asignarse al UE mientras dure la llamada de emergencia. Algunas de estas funciones (por ejemplo, gestión ESRD/ESRK) pueden no ser consideradas como parte de SUPL y pueden ser admitidas en una entidad física o lógica separada que pueda ser consultada por E-SLP 272 (por ejemplo, como se describe en la solución NENA I2). El ESRD y el ESRK corresponden a los mismos números de directorio nombrados usados para la admisión de llamadas de emergencia en modo circuito (por ejemplo, J-STD-036). El ESRD y el ESRK también corresponden al ESRN y al ESQK, respectivamente, descritos en la solución NENA I2.

[66] En la etapa 13, E-SLP 272 devuelve a E-CSCF 254 una respuesta de encaminamiento (o una respuesta de ubicación de emergencia) que puede incluir (a) la identidad del PSAP (que puede ser una URL de SIP o una dirección IP) si el PSAP 180 admite IP o (b) ESRD y ESRK si el PSAP 180 admite PSTN. La respuesta de encaminamiento también puede incluir la estimación de la posición provisional para el UE 110 si así lo solicita la E-CSCF 254. E-SLP 272 puede almacenar para el UE 110 un registro de llamadas que contenga toda la información recopilada para el UE.

[67] Las etapas 14a y 15a se realizan si el PSAP 180 admite IP. En la etapa 14a, el E-CSCF 254 encamina el SIP INVITAR (recibido en la etapa 5) al PSAP 180. El SIP INVITAR puede incluir una estimación de posición provisional y posiblemente la identidad o dirección para el UE 110 y la dirección IP o nombre de E-SLP 272. En la etapa 15a, se puede intercambiar señalización SIP adicional para establecer la llamada de emergencia.

[68] Las etapas 14b, 14c y 15b se realizan si el PSAP 180 admite PSTN. En la etapa 14b, el E-CSCF 254 envía el SIP INVITAR a través de una función de control de puerta de enlace de salida (BGCF) a MGCF 258. El SIP INVITAR puede incluir el número de devolución de llamada (por ejemplo, MSISDN o MDN) para el UE 110 y/o puede incluir el ESRD y ESRK (pero posiblemente no una estimación de posición provisional). En la etapa 14c, el MGCF 258 encamina la llamada de emergencia al PSAP 180 a través de la PSTN, posible a través de un encaminador selectivo, utilizando SS7 ISUP y/o señalización MF. El ESRD o ESRK pueden usarse como números de encaminamiento y el ESRK y/o el número de devolución de llamada se pasan al PSAP 180 (por ejemplo, a través de señalización MF CAMA) como la identidad del UE 110 y como una clave para obtener más información. En la etapa 15b, puede intercambiarse señalización SIP adicional y puede producirse el interfuncionamiento con SS7 ISUP y/o MF en MGCF 258 para establecer la llamada de emergencia.

[69] La ruta de llamada para un PSAP compatible con IP y un PSAP compatible con PSTN se establece por separado. Para un PSAP compatible con PSTN, el interfuncionamiento entre VoIP (por ejemplo, RTP/IP) y el modo de circuito (por ejemplo, PCM) se produce en una pasarela de medios (MGW) controlada por MGCF 258. Para un PSAP compatible con IP, la ruta de la llamada sería IP de extremo a extremo e iría entre el UE 110 y el PSAP 180, posiblemente en parte a través de Internet pública o una red de IP privada, pero omitiría cualquier MGW.

[70] En la etapa 16, después de que se establece la llamada, el PSAP 180 puede enviar una solicitud de ubicación al E-SLP 272, que puede identificarse por una dirección IP o nombre obtenido en la etapa 14a o un ESRK obtenido en la etapa 14c. El PSAP 180 identifica el UE 110 usando la dirección de usuario pública del UE (si el PSAP 180 admite IP) o un número de devolución de llamada u otra dirección (por ejemplo, MSISDN o MDN) o el ESRK (si el PSAP 180 admite PSTN). La solicitud de ubicación indica un requisito para una estimación de posición precisa. Para una llamada de VoIP de emergencia en los Estados Unidos, la solicitud de ubicación puede ser idéntica a una solicitud de posición de servicios de emergencia en J-STD-036 si el PSAP 180 admite PSTN y puede ser una extensión de este mensaje si el PSAP 180 admite IP. Para una llamada de VoIP de emergencia en algunas otras regiones del mundo, la solicitud de ubicación puede ser idéntica a una solicitud inmediata de ubicación de emergencia definida para OMA MLP.

[71] En la etapa 17, E-SLP 272 puede seleccionar una V-SLP si las capacidades de ubicación de la E-SLP 272 no se extienden al área geográfica donde se informó la última posición conocida del UE 110 o si el uso de una V-SLP puede proporcionar una ubicación más precisa y fiable. La E-SLP 272 puede obtener una dirección V-

SLP desde la posición más reciente del UE 110 y/o desde la dirección V-SLP más reciente proporcionada por el E-CSCF 254. Con el fin de asegurar la V-SLP correcta, la E-SLP 272 puede consultar la ubicación del UE 110 y/o la dirección V-SLP de E-CSCF 254 (no mostrada en la FIG. 5) si E-CSCF 254 no transfiere automáticamente esta información después de cualquier nuevo registro del UE 110 en la etapa 4. La E-SLP 272 puede entonces abrir una nueva transacción SUPL con el UE 110 enviando un SUPL INIT directamente al UE usando IP con terminación móvil o UDP/IP (en cuyo caso se puede omitir la etapa 18) o enviando un mensaje inmediato que contiene el SUPL INIT a E-CSCF 254. El SUPL INIT puede incluir los parámetros descritos anteriormente para la etapa 7.

[72] En la etapa 18, E-CSCF 254 transfiere al UE 110 el SUPL INIT dentro de un mensaje IMS inmediato, algún otro mensaje IMS, un mensaje SIP (por ejemplo, otro INVITAR), o algún otro mensaje basado en IP que usa las asociaciones IP seguras entre E-CSCF 254, P-CSCF 252 y el UE 110.

[73] En la etapa 19, el UE 110 establece una conexión segura de IP a E-SLP 272. El UE 110 puede entonces intercambiar mensajes SUPL con E-SLP 272 para modo proxy o con E-SPC 414 o V-SPC 424 para modo no proxy (similar a las etapas 9, 10 y 11) para obtener una estimación de posición precisa para el UE.

[74] En la etapa 20, la E-SLP 272 envía la estimación precisa de la posición para el UE 110 en una respuesta de ubicación al PSAP 180. Para una llamada de emergencia en los EE. UU., la respuesta de ubicación puede ser idéntica a un mensaje de respuesta de posición de servicios de emergencia en J-STD-036 para la interfaz E2 si el PSAP 180 es compatible con PSTN (y, de este modo, puede incluir información adicional como el MSISDN del UE 110). Para una llamada de emergencia en algunas otras regiones del mundo, la respuesta de ubicación puede ser idéntica a una respuesta inmediata de ubicación de emergencia definida para OMA MLP.

[75] El UE 110 puede comunicarse después con el PSAP 180 para la llamada de VoIP de emergencia. Cuando se libera la llamada más tarde, E-CSCF 254 puede enviar una indicación a E-SLP 272, que luego puede liberar cualquier registro de la llamada. La E-CSCF 254 o el UE 110 también pueden anular el registro del ID de usuario público de emergencia, que se registró en las etapas 2 a 4. De forma alternativa, E-CSCF 254, E-SLP 272 y el UE 110 pueden permitir que el registro y los registros de llamadas permanezcan durante un cierto período de tiempo para admitir una posible devolución de llamada posterior desde el PSAP 180 al UE 110 y/o solicitudes de ubicación adicionales.

1.2. Acceso

[76] Para la etapa 1, el UE 110 puede conectarse a una red de acceso a través del acceso GPRS, el acceso cdma2000 o el acceso WLAN. La etapa 1 se puede realizar de diferentes maneras para diferentes tipos de acceso.

[77] Para el acceso GPRS, el UE 110 puede realizar la conexión GPRS para conectarse a una red de acceso 3GPP y puede realizar la activación del contexto del Protocolo de Datos por Paquetes (PDP) GPRS para establecer conectividad IP en SGSN 232a y GGSN 232b, como se describe en TR 23.867 y TS 23.060 de 3GPP. Se puede usar una indicación de emergencia en la conexión GPRS y/o un nombre de punto de acceso (APN) global para servicios de emergencia para la activación del contexto PDP, lo que puede garantizar la provisión de un GGSN y un P-CSCF en la V-PLMN 130. P-CSCF 252 puede ser un P-CSCF en una PLMN GPRS de servicio como se proporciona durante la activación del contexto PDP.

[78] Para el acceso WLAN 3GPP, el UE 110 puede realizar un procedimiento WLAN AAA para conectarse a una WLAN y puede realizar el establecimiento de un túnel I-WLAN para conectividad IP a PDG 236. El UE 110 puede seleccionar el servicio de la V-PLMN 130 usando un identificador de acceso de red itinerante (NAI) que indica tanto la H-PLMN 160 como la V-PLMN 130 en la solicitud de autenticación y autorización. El NAI itinerante se describe en TS 23.234 y TS 23.003 de 3GPP. Esto asegura que el UE 110 puede obtener acceso IP a servicios IMS desde PDG 236 en la V-PLMN 130 en lugar de desde un PDG en la H-PLMN 160 (que puede restringir el acceso a PSAP si la H-PLMN 160 es remota). Se puede usar un WLAN APN (W-APN) global para servicios de emergencia para la detección de PDG y el establecimiento de túneles. Este servicio puede usar un identificador de red externo único global (para admitir servicios de emergencia) y la identidad de V-PLMN. P-CSCF 252 puede ser una P-CSCF en una V-PLMN asociada con una WLAN y puede ser descubierta a través de una consulta DNS en el W-APN.

[79] Para el acceso cdma2000, el UE 110 obtiene una dirección IP simple en lugar de una dirección IP móvil ya que el servicio se obtiene de la V-PLMN 130 y no de la H-PLMN 160. De forma alternativa, el UE 110 puede obtener una dirección IP móvil desde la V-PLMN 130 en lugar de desde la H-PLMN 160, como es más normal para una dirección IP móvil. Una dirección IP puede ser una dirección IPv4 o una dirección IPv6. Si el UE 110 no ha establecido conectividad (por ejemplo, no tiene una dirección IP asignada), entonces el UE 110 puede establecer una sesión de protocolo punto a punto (PPP) y realizar cualquier autenticación y autorización con la PDSN 242 en la V-PLMN 130, como se describe en X.P0011D y TIA-835-D de 3GPP. El UE 110 puede obtener una dirección IP simple, por ejemplo, usando el protocolo de control de protocolo de Internet PPP (IPCP). Si el

UE 110 ya ha establecido conectividad IP y tiene una sesión PPP a PDSN 242 pero se le asigna una dirección o direcciones IP móviles en H-PLMN 160 en lugar de una dirección o direcciones IP simples, entonces el UE 110 puede finalizar cualquier sesión de paquetes asociada con estas direcciones IP así como también cualquier registro IMS si el UE 110 no es compatible con direcciones IP simples IP e IP móviles simultáneas, que es una capacidad de UE opcional pero no obligatoria en TIA-835D. El UE 110 puede entonces obtener una dirección IP simple como se describe en TIA-835D. Si el UE 110 puede admitir direcciones IP simples y móviles simultáneas, entonces el UE 110 puede obtener simplemente una dirección IP simple si aún no tiene una.

[80] Para el acceso cdma2000, el UE 110 puede descubrir una dirección P-CSCF en la V-PLMN 130 mediante (a) el uso de DHCP o IPCP para obtener un nombre de dominio P-CSCF y una dirección DNS de un servidor DHCP o PDSN 242 y luego (b) usando el DNS para obtener una o más direcciones IP P-CSCF del servidor DNS. Si el UE 110 se mueve y accede a una nueva RAN, entonces la V-PLMN 130 y el UE 110 pueden emplear un procedimiento de transferencia rápida descrito en TIA-835-D si se necesita un nuevo PDSN objetivo y ya se ha establecido una llamada de VoIP de emergencia. Esto evita la necesidad de terminar y restablecer la llamada.

[81] Para el acceso WLAN 3GPP2, el UE 110 puede realizar procedimientos de acceso WLAN existentes que incluyen AAA, adquisición de direcciones IP y descubrimiento de un encaminador IP predeterminado y una dirección de servidor DNS (por ejemplo, a través del DHCP). El UE 110 puede entonces acceder a una PDIF en una PLMN que admite llamadas de emergencia desde la ubicación geográfica de la WLAN a la que accede el UE 110. La WLAN puede anunciar redes cdma2000 asociadas de modo que se puedan distinguir las llamadas de emergencia que admiten las PLMN. Este anuncio se puede lograr, por ejemplo, enviando identificadores de conjunto de servicios (SSID) asociados en tramas de baliza IEEE 802.11 o mediante respuestas a tramas de solicitud de sondas de UE. Las PLMN se pueden priorizar según el orden en que se anuncian, mediante el uso de un indicador para cada PLMN anunciada, o asegurando (por ejemplo, exigiendo) que todas las PLMN anunciadas admitan llamadas de emergencia. Para el acceso WLAN inicial, AAA y adquisición de dirección IP, el UE 110 puede elegir una PLMN (por ejemplo, un SSID) que esté implícita o indicada para admitir llamadas de emergencia.

[82] Después del acceso WLAN inicial, AAA, adquisición de dirección IP y descubrimiento de un encaminador predeterminado y dirección del servidor DNS, el UE 110 puede crear un nombre de dominio completo (FQDN) que indique el servicio IMS y use un dominio asociado con una de las PLMN anunciadas por la WLAN que admite llamadas de emergencia. El UE 110 puede entonces usar el FQDN para descubrir la dirección o direcciones IP de una o más PDIF del servidor DNS. El UE puede elegir una PDIF y establece un túnel IPsec a la misma usando los procedimientos descritos en X.S0028-200 de 3GPP2. Esto proporciona al UE 110 una segunda dirección IP interna, que puede usarse para procedimientos posteriores relacionados con IMS.

[83] Tras el establecimiento del túnel a una PDIF desde una WLAN, el UE 110 puede descubrir una dirección P-CSCF de la misma manera que un UE accediendo a una PDSN desde una red de acceso cdma2000 (por ejemplo, a través de DHCP para obtener una dirección de servidor DNS y un nombre de dominio y luego a través del DNS para obtener la dirección IP de P-CSCF). En este caso, la PDIF puede actuar como un agente de retransmisión DHCP en lugar del PDSN. El descubrimiento de las direcciones PIDF y P-CSCF a través del DNS puede incluir una indicación (por ejemplo, en el nombre proporcionado al servidor DNS) de que se necesita admitir una llamada de emergencia.

[84] Si el UE 110 ya tiene una asociación (por ejemplo, un túnel) a una PDIF en una PLMN inadecuada y si el UE 110 no admite túneles a diferentes PDIF simultáneamente, entonces el UE 110 puede liberar cualquier sesión de paquetes admitida a través de la PDIF actual y liberar el túnel a la PDIF antes de seleccionar y establecer un túnel a una nueva PDIF en una nueva PLMN adecuada.

[85] Después de una conexión de red de acceso cdma2000 o WLAN, el UE 110 puede descubrir una dirección SUPL V-SLP usando una consulta DNS con un nombre de dominio V-PLMN conocido y una identificación V-SLP (por ejemplo, supl_vslp@nombre_dominio).

[86] El flujo de mensajes 500 tiene las siguientes adiciones de características relacionadas con OMA SUPL versión 1.0.

(a) Adición de una dirección E-SLP en un SUPL INIT, que anula y reemplaza una dirección H-SLP configurada en el UE 110.

(b) Interfaz entre el lado IMS (por ejemplo, E-CSCF 254) y el lado de la ubicación (por ejemplo, E-SLP 272).

(c) Uso de V-SLP 274 y descubrimiento de la dirección V-SLP.

(d) Transmisión de un SUPL INIT usando IP con terminación móvil, UDP/IP, señalización SIP o IMS, en lugar de SMS o WAP Push, para reducir el retardo.

(e) Adición de una indicación de servicios de emergencia en SUPL INIT.

(f) Preferencia por la adición de nuevas mediciones de ubicación en POS INIT SUPL.

(g) Uso del protocolo ILP entre E-CSCF 254 y E-SLP 272, que puede ser similar al RLP existente.

(h) Seguridad.

2. Llamada de VoIP de emergencia con plano de control 3GPP

[87] **La FIG. 6** muestra un diagrama de bloques de un modo de realización de una arquitectura de red 600 aplicable para la ubicación del plano de control 3GPP. Para simplificar, la FIG. 6 solo muestra entidades e interfaces relevantes para admitir llamadas de VoIP de emergencia con acceso GPRS y ubicación del plano de control 3GPP.

[88] La red de acceso 120 puede ser una GERAN o una UTRAN. La V-PLMN 130 puede incluir P-CSCF 252, E-CSCF 254 y MGCF 258 para admitir IMS (por ejemplo, VoIP), SGSN/GGSN 232 para servicios conmutados por paquetes y GMLC 276 para servicios de ubicación. El GMLC 276 reemplaza al E-SLP 272 y es una versión mejorada del GMLC descrito en 23.271 de 3GPP, Versión 6. La V-PLMN 130 también puede incluir E-SLP 272 y V-SLP 274 para servicios de ubicación (no mostrados en la FIG. 6).

[89] En un modo de realización, el GMLC 276 se comunica con E-CSCF 254 a través de la interfaz Li y se comunica con el PSAP 180 a través de la interfaz J-STD-036 E2'. El uso de la misma interfaz Li para GMLC 276 y E-SLP 272 puede ocultar diferencias de arquitectura de ubicación entre SUPL y el plano de control 3GPP de E-CSCF 254. De forma similar, el uso de la misma interfaz J-STD-036 E2' para GMLC 276 y E-SLP 272 puede ocultar diferencias de arquitectura de ubicación del PSAP 180. Las otras interfaces de la FIG. 6 son conocidas en la técnica.

2.1. Configuración de llamada

[90] **La FIG. 7** muestra un modo de realización de un flujo de mensajes 700 para la configuración de llamadas de VoIP de emergencia usando un plano de control 3GPP. Para mayor claridad, las entidades que son menos relevantes (por ejemplo, la red de acceso 120, P-CSCF 252, S/R 292) se omiten en la FIG. 7 pero están incluidas en las descripciones a continuación. El flujo de mensajes 700 supone que el UE 110 tiene una UICC y que existe un acuerdo de itinerancia entre H-PLMN 160 y V-PLMN 130.

[91] En la etapa 1, el UE 110 realiza una conexión GPRS con una indicación de servicios de emergencia, si el UE todavía no está conectado a GPRS. La conexión GPRS puede implicar obtener acceso al SGSN 232a, realizar cualquier autenticación y descarga de datos de suscripción de HLR/HSS 266 en H-PLMN 160 a SGSN 232a, y así sucesivamente. En la etapa 2, el UE 110 realiza la activación del contexto PDP usando el APN global para servicios de emergencia. El contexto PDP se asigna a un GGSN local en V-PLMN 130 (por ejemplo, y no a una GGSN en H-PLMN 160). El UE 110 obtiene una dirección IP y puede descubrir una dirección de servidor SIP local (por ejemplo, P-CSCF 252) durante la activación del contexto PDP.

[92] En la etapa 3, el SGSN 232 toma conocimiento del inicio de una llamada de emergencia basándose en la indicación de emergencia de la etapa 1 o en el APN global para servicios de emergencia de la etapa 2. El SGSN 232a puede entonces iniciar una solicitud de ubicación inducida por red conmutada por paquetes (PS-NI-LR) descrita en TS 23.271 de 3GPP para obtener una estimación de posición provisional o una estimación de posición más precisa para el UE 110. La PS-NI-LR proporciona una respuesta más rápida que si el SGSN 232 espera una solicitud para obtener la estimación de posición (por ejemplo, a través de una MAP PSL en la etapa 17) del GMLC 276. La PS-NI-LR puede ser realizada por un SGSN inicial. Si el UE 110 se transfiere a un nuevo SGSN, entonces el nuevo SGSN no necesita realizar otra PS-NI-LR. En la etapa 4, una vez que se obtiene una estimación de posición para el UE 110, el SGSN 232 puede determinar una dirección GMLC (por ejemplo, desde la ID de célula actual) y puede enviar al GMLC 276 un informe de ubicación de suscriptor (SLR) que contiene la estimación de posición, identidad del UE y/u otra información. La identidad del UE puede ser una identidad internacional de abonado móvil (IMSI), un número ISDN de abonado móvil (MSISDN), una identidad internacional de equipo móvil (IMEI), un número de serie electrónico (ESN), un identificador de equipo móvil (MEID) u otra identidad. Si se realiza la etapa 4, entonces se pueden omitir las etapas 10 y 11.

[93] En la etapa 5, el UE 110 envía un SIP REGISTRAR a P-CSCF 252, que se descubrió en la etapa 2. El SIP REGISTRAR puede incluir la información descrita anteriormente para la etapa 2 en la FIG. 5 y también puede incluir la dirección del SGSN si deben realizarse las etapas 10 y 11. Debido a la presencia de la indicación de servicios de emergencia o el ID de usuario público de emergencia, P-CSCF 252 envía el SIP REGISTRAR a E-CSCF 254 en la misma red. La etapa 5 se puede realizar en paralelo con la etapa 3. En la etapa 6, E-CSCF

254 envía el SIP REGISTRAR a H-PLMN 160 donde se produce el registro IMS normal, similar a la etapa 3 en la FIG. 5.

[94] En la etapa 7, después de que H-PLMN 160 devuelve un 200 OK a E-CSCF 254, se devuelve un 200 OK al UE 110. El UE 110 también puede volver a registrarse si hay un traspaso a un SGSN diferente dentro de la V-PLMN 130. Si el UE 110 se vuelve a registrar utilizando su ID de usuario público de emergencia, E-CSCF 254 puede transferir cualquier nueva información de ubicación y/o cualquier nueva dirección del SGSN al GMLC 276.

[95] Al igual que en la FIG. 5, en un modo de realización alternativo de las etapas 5, 6 y 7, después de que el UE 110 envíe un SIP REGISTRAR a P-CSCF 252 en la etapa 5, P-CSCF 252 puede reenviar el SIP REGISTRAR directamente a S-CSCF 264 o I-CSCF 262 en H-PLMN 160 y eludir E-CSCF 254 en V-PLMN 130. En este caso, un SIP 200 OK de H-PLMN 160 se devolvería a P-CSCF 252 en lugar de a E-CSCF 254, y P-CSCF 252 devolvería el 200 OK al UE 110 en la etapa 7. Este modo de realización alternativo puede reducir o evitar impactos especiales a P-CSCF 252 para admitir llamadas de emergencia de VoIP porque las acciones P-CSCF 252 son entonces similares a las del registro normal.

[96] En la etapa 8, el UE 110 envía a P-CSCF 252 un SIP INVITAR que puede incluir la información descrita anteriormente para la etapa 5 en la FIG. 5. P-CSCF 252 envía el SIP INVITAR a E-CSCF 254.

[97] En la etapa 9, en base a la admisión del UE del plano de control 3GPP para el modo de paquetes, la E-CSCF 254 envía una solicitud de encaminamiento al GMLC 276 indicada por la célula servidora u otra información de ubicación recibida en la etapa 8. La solicitud de encaminamiento puede incluir la información descrita en la etapa 6 de la FIG. 5 así como la dirección del SGSN si se proporciona durante el registro. E-CSCF 254 puede seleccionar el GMLC 276, un servidor genérico de ubicación capaz de actuar como un GMLC, o algunos otros tipos de servidor (por ejemplo, una SLP). El servidor de ubicación seleccionado puede elegir usar un plano de control 3GPP basándose en las capacidades de ubicación del UE transferidas por E-CSCF 254. La E-CSCF 254 puede solicitar información de ubicación del GMLC 276 y/o la selección de un PSAP correspondiente a la información de ubicación disponible y el tipo de servicio de emergencia que se solicita.

[98] El GMLC 276 avanza a la etapa 12 si la información de ubicación proporcionada en la etapa 9 permite que el GMLC 276 obtenga una estimación de posición para el UE 110 que sea lo suficientemente precisa como para cumplir la solicitud en la etapa 9. El GMLC 276 también puede esperar hasta recibir el MAP SLR del SGSN 232 en la etapa 4 y, si se obtiene una estimación de posición adecuada, proceder a la etapa 12. De lo contrario, se realizan las etapas 10 y 11 para obtener una estimación de posición adecuada para el UE 110.

[99] En la etapa 10, el GMLC 276 envía al SGSN 232 un MAP para proporcionar la ubicación del abonado (PSL) que contiene la precisión/retardo de QoP para una estimación rápida de la posición intermedia. Si no se realiza la etapa 4, entonces el GMLC 276 puede determinar el SGSN 232 a partir de cualquier dirección explícita o información de ubicación (por ejemplo, ID de célula) recibida en la etapa 9. Si no se recibió tal información o si el SGSN inicialmente elegido es incorrecto (respuesta de error recibida en la etapa 11), entonces el GMLC 276 puede consultar un HSS indicado por el IMSI o pseudo IMSI o MSISDN del UE para obtener la dirección del SGSN. En la etapa 11, el SGSN 232 puede devolver una estimación de posición obtenida en la etapa 3, esperar hasta que se complete la etapa 3 y luego devolver la estimación de posición, u obtener una estimación de posición de la RAN y luego devolver la estimación de posición al GMLC 276.

[100] En la etapa 12, el GMLC 276 selecciona un PSAP basándose en la estimación de posición. La siguiente descripción supone que el PSAP 180 es el PSAP seleccionado. Si el PSAP 180 admite PSTN, entonces el GMLC 276 obtiene un número de directorio ESRD no marcable que se puede usar para encaminar a PSAP 180 y un número de directorio ESRK no marcable que identifica el PSAP 180, el GMLC 276 y, temporalmente, el UE 110.

[101] En la etapa 13, el GMLC 276 devuelve a E-CSCF 254 una respuesta de encaminamiento que puede incluir la información descrita anteriormente para la etapa 13 en la FIG. 5. En la etapa 14, la llamada de emergencia se envía al PSAP 180, como se describe para las etapas 14a, 14b y 14c en la FIG. 5. En la etapa 15, el resto de la configuración de la llamada de emergencia procede como se describe para las etapas 15a y 15b en la FIG. 5. En la etapa 16, el PSAP 180 envía una solicitud de ubicación al GMLC 276, que se indica en la etapa 14 mediante una dirección/nombre IP o un ESRK, como se describe para la etapa 16 en la FIG. 5.

[102] En la etapa 17, el GMLC 276 envía un MAP PSL al SGSN 232 solicitando una ubicación precisa. El GMLC 276 puede obtener la dirección del SGSN a partir de la información de ubicación más reciente para el UE 110 o a partir de una actualización de la dirección del SGSN de la E-CSCF 254. El GMLC 276 también puede consultar la dirección del SGSN desde E-CSCF 254 si esta dirección se recibe en mensajes para REGISTRAR de nuevo pero no se transfiere. El GMLC 276 también puede consultar la dirección del SGSN desde el HSS indicado por IMSI o pseudo IMSI o MSISDN del UE. En la etapa 18, el SGSN 232 instiga el posicionamiento del UE 110 por la RAN. En la etapa 19, el SGSN 232 devuelve la estimación de posición al GMLC 276. En la etapa

20, el GMLC 276 devuelve la estimación de posición al PSAP 180, como se describe para la etapa 20 en la FIG. 5.

[103] El UE 110 puede comunicarse después con el PSAP 180 para la llamada de VoIP de emergencia. Cuando se libera la llamada más tarde, la E-CSCF 254 puede enviar una indicación al GMLC 276, que luego puede liberar cualquier registro de la llamada. La E-CSCF 254 o el UE 110 también pueden anular el registro del ID de usuario público de emergencia, que se registra en las etapas 5 a 7. De forma alternativa, la E-CSCF 254, el GMLC 276 y el UE 110 pueden permitir que el registro y los registros de llamadas permanezcan durante un cierto período de tiempo para admitir una posible devolución de llamada posterior desde el PSAP 180 al UE 110 y/o solicitudes de ubicación adicionales.

[104] El flujo de mensajes 700 realiza la configuración de llamadas y la ubicación para el UE 110 de una manera coordinada y tiene las siguientes características.

(a) El SGSN 232 puede obtener la ubicación del UE y enviarla al GMLC 276 siempre que el contexto PDP esté activado y/o si el GMLC 276 lo solicita.

(b) El GMLC 276 puede recibir una dirección SIP-URI pública para el UE 110 de E-CSCF 254.

(c) Si el PSAP 180 admite PSTN, el GMLC 276 y la E-CSCF 254 pueden transferir información al PSAP 180 (por ejemplo, un ESRK de 10 dígitos) usado para identificar tanto la llamada como el GMLC 276. Esta información permite que el PSAP 180 extraiga la ubicación y otra información (por ejemplo, MSISDN, URI del SIP) del GMLC 276.

(d) La interfaz Li entre E-CSCF 254 y un servidor de ubicación (por ejemplo, E-SLP 272) se puede usar para admitir llamadas de emergencia desde una I-WLAN cuando se usa SUPL como procedimiento de posición. El uso de la misma interfaz Li para UMTS, GPRS e I-WLAN permite que el IMS (por ejemplo, la E-CSCF 254) funcione sin tener que estar al tanto de la solución de ubicación, lo que puede simplificar el manejo del IMS.

(e) Si el UE 110 no admite la ubicación por la RAN (por ejemplo, admite SUPL pero no el plano de control 3GPP), entonces el SGSN 232 puede omitir la PS-NI-LR.

(f) El PSAP 180 puede tener requisitos de ubicación específicos que el SGSN 232 puede desconocer, por ejemplo, precisión particular o incluso no admitir coordenadas de ubicación (por ejemplo, si el PSAP 180 admite E911 fase 0 o 1). Dichos requisitos son compatibles con el GMLC 276 para llamadas de emergencia con conmutación de circuitos.

[105] La interfaz Li se puede usar para lograr las características enumeradas anteriormente. Admitir la interfaz Li externamente puede no ser necesario si las funciones del GMLC y la E-CSCF son compatibles con la misma plataforma. La interfaz Li puede extenderse al uso entre cualquier entidad IMS y el GMLC para admitir otras características asociadas con servicios basados en IP e IMS, como se describió anteriormente para SUPL.

[106] El SGSN 232 se puede seleccionar basándose en una estimación de posición provisional (por ejemplo, célula de servicio) para el UE 110. El GMLC 276 se puede seleccionar mediante E-CSCF 254 basándose en la misma estimación de posición provisional. La estimación de la posición provisional puede ser empujada desde el SGSN 232 al GMLC 276 o ser extraída por el GMLC 276 desde el SGSN 232. Una entidad puede determinar la otra entidad de la siguiente manera.

[107] El SGSN 232 puede empujar la estimación de la posición provisional al GMLC 276. El SGSN 232 puede obtener esta estimación de posición provisional a través de la PS-NI-LR, determinar una dirección del GMLC según la ubicación actual del UE (por ejemplo, la ID de la célula actual) y enviar/empujar la estimación de posición al GMLC 276 usando un informe de ubicación de abonado (SLR) MAP. La E-CSCF 254 puede consultar el GMLC 276 una dirección del PSAP con el fin de encaminar la llamada de emergencia. El GMLC 276 puede esperar (si es necesario) al MAP SLR del SGSN 232 para determinar la dirección del PSAP a partir de la estimación de la posición provisional.

[108] El GMLC 276 puede extraer la estimación de la posición provisional del SGSN 232. El SGSN 232 aún puede realizar la PS-NI-LR pero no enviaría la estimación de posición al GMLC 276 hasta que el GMLC solicite la estimación de la posición a través de una solicitud MAP PSL. El GMLC 276 puede determinar la dirección del SGSN usando uno de los siguientes.

(a) El GMLC 276 consulta la dirección del SGSN desde el HSS 266 en la H-PLMN 160 (si el UE 180 tiene UICC y se admite la itinerancia en la V-PLMN 130) o el HSS 250 en la V-PLMN 130 (si el UE 180 no tiene UICC o no hay acuerdo de itinerancia en la V-PLMN 130).

(b) El UE 110 incluye la dirección del SGSN actual o información de la ubicación (por ejemplo, una ID de célula GPRS) de la cual se puede obtener la dirección del SGSN en cada mensaje REGISTRAR y volver a REGISTRAR enviado al IMS o en cada mensaje SIP INVITAR enviado al IMS para una llamada de emergencia. La E-CSCF 254 luego transfiere la dirección del SGSN o la información de ubicación al GMLC 276. El UE 110 se vuelve a registrar en el IMS después de cualquier traspaso entre SGSN.

3. Llamada de VoIP de emergencia con X.S0024

[109] **La FIG. 8** muestra un diagrama de bloques de un modo de realización de una arquitectura de red 800 aplicable para la ubicación X.S0024 para redes cdma2000. La red de acceso 120 puede comprender una red CDMA2000 1X, una red CDMA2000 1xEV-DO, una red WLAN 3GPP2, y así sucesivamente. La V-PLMN 130 puede incluir P-CSCF 252, E-CSCF 254 y MGCF 258 para admitir el IMS (por ejemplo, VoIP) y el PDSN 242 para servicios con conmutación de paquetes (no mostrados). La V-PLMN 130 puede incluir E-PS 282 y V-PS/PDE 284 (como se muestra) y también puede incluir E-SLP 272 y V-SLP 274 (no mostrada) para servicios de ubicación. El E-PS 282 sustituye a un H-PS para la ubicación de las llamadas de emergencia. El E-PS 282 y el V-PS/PDE 284 pueden residir en otras redes.

[110] En un modo de realización, el UE 110 se comunica con el E-PS 282 a través de una interfaz LCS-x y se comunica con el V-PS/PDE 284 a través de una interfaz LCS-y. El E-PS 282 se comunica con el V-PS/PDE 284 a través de una interfaz LCS-z, se comunica con E-CSCF 254 a través de una interfaz LCS-i, y se comunica con el PSAP 180 a través de la interfaz J-STD-036 E2'. La interfaz LCS-i puede ser similar a la del RLP o Li/ILP para SUPL, la interfaz v2 en la solución NENA I2, o alguna otra interfaz. El protocolo para la interfaz LCS-i puede ser ILP usado para SUPL. Las interfaces LCS-x, LCS-y y LCS-z se describen en X.S0024.

3.1. Configuración de llamada

[111] **La FIG. 9** muestra un modo de realización de un flujo de mensajes 900 para la configuración de llamadas de VoIP de emergencia usando X.S0024. En la etapa 1, el UE 110 descubre y se conecta a una red de acceso, establece conectividad IP y puede descubrir un servidor SIP local (por ejemplo, la P-CSCF 252), como se describió anteriormente para la etapa 1 en la FIG. 5. Después la conexión a la red de acceso, el UE 110 puede descubrir una dirección del V-PS usando una consulta DNS con un nombre de dominio [domain name] de V-PLMN conocido y una identificación del V-PS (por ejemplo, xs0024__vps@domain_name).

[112] En la etapa 2, el UE 110 envía un SIP REGISTRAR a la P-CSCF 252, que reenvía el mensaje a la E-CSCF 254. En la etapa 3, la E-CSCF 254 reenvía el SIP REGISTRAR a H-PLMN 160 donde se produce el registro del IMS normal. En la etapa 4, la E-CSCF 254 (por ejemplo, después de recibir un 200 OK de H-PLMN 160) devuelve un 200 OK al UE 110. El UE 110 puede volver a registrarse si se transfiere a un PCF, PDSN o WLAN diferente dentro de la misma V-PLMN.

[113] En un modo de realización alternativo de las etapas 2, 3 y 4, después de que el UE 110 envíe un SIP REGISTRAR a la P-CSCF 252 en la etapa 2, la P-CSCF 252 puede reenviar el SIP REGISTRAR directamente a la S-CSCF 264 o la I-CSCF 262 en la H-PLMN 160 y omitir la E-CSCF 254 en la V-PLMN 130. En este caso, un SIP 200 OK de H-PLMN 160 se devolvería a P-CSCF 252 en lugar de a E-CSCF 254, y P-CSCF 252 devolvería el 200 OK al UE 110 en la etapa 4. Este modo de realización alternativo puede reducir o evitar impactos especiales a P-CSCF 252 para admitir llamadas de emergencia de VoIP porque las acciones P-CSCF 252 son entonces similares a las del registro normal.

[114] En la etapa 5, el UE 110 envía un SIP INVITAR a la P-CSCF 252 (no mostrado), que envía el SIP INVITAR a la E-CSCF 254. En la etapa 6, la E-CSCF 254 puede determinar que el UE 110 admite X.S0024 y envía una solicitud de encaminamiento al E-PS 282 en la misma red o en una red diferente. La solicitud de encaminamiento puede incluir la información descrita anteriormente para la etapa 6 en la FIG. 5 y la dirección del V-PS si se obtiene durante el registro.

[115] El E-PS 282 continúa a la etapa 12 si la información de ubicación proporcionada en la etapa 6 permite que el E-PS 282 obtenga una estimación de posición suficientemente precisa para el UE 110. De lo contrario, las etapas 7 a 11 se realizan para obtener una estimación de posición adecuada para el UE 110. En la etapa 7, el E-PS 282 actúa como un H-PS en la realización de la siguiente ubicación X.S0024 usando procedimientos similares a los de (a) admitir itinerancia X.S0024 si se seleccionó un V-PS o (b) no admitir itinerancia X.S0024 si no se seleccionó un V-PS. El E-PS 282 genera un SUPL INIT X.S0024 para iniciar un procedimiento de ubicación iniciado por la red con el UE 110. El E-PS 282 puede enviar el SUPL INIT directamente al UE 110 usando un IP con terminación móvil o UDP/IP, en cuyo caso se omite la etapa 8. El E-PS 282 también puede enviar SUPL INIT dentro de un mensaje inmediato a la E-CSCF 254. En cualquier caso, el SUPL INIT puede incluir el modo de posicionamiento, la precisión/retardo de la QoP para una estimación rápida de la posición intermedia, una dirección IP del E-PS, una indicación de llamada de emergencia, y así sucesivamente. Cualquier dirección del E-PS transmitida en SUPL INIT anula cualquier dirección del H-PS configurada en UE 110.

[116] En la etapa 8, la E-CSCF 254 envía el SUPL INIT al UE 110 a través de la P-CSCF 252 usando la señalización IMS o SIP. En la etapa 9, el UE 110 establece una conexión de IP segura al E-PS 282, que puede ser el H-PS para el UE 110 o puede haber incluido su dirección IP en el SUPL INIT en la etapa 7. El UE 110 envía entonces al E-PS 110 un SUPL INICIO que puede incluir las capacidades de ubicación del UE, la información de ubicación para el UE 110, una estimación de posición para el UE 110 (si está disponible), y así sucesivamente. El E-PS 282 puede pasar a la etapa 12 y finalizar la transacción de ubicación con el UE 110 enviando un SUPL FIN si se recibe una estimación de posición con precisión suficiente para determinar un PSAP del UE 110 en la etapa 9.

[117] En la etapa 10, el E-PS 282 determina una PDE local adecuada o un V-PS remoto adecuado para realizar el posicionamiento basándose en la información de ubicación recibida en la etapa 9 u otra información de ubicación recibida en la etapa 6. El E-PS 282 también decide si usar el modo proxy o no proxy. El E-PS 282 luego interactúa con el V-PS o la PDE para el posicionamiento y envía al UE 110 una SUPL RESPUESTA X.S0024 que puede incluir una dirección IP de la PDE si se selecciona el modo no proxy. En la etapa 11, el UE 110 intercambia mensajes POS SUPL con la PDE para el modo no proxy o con el E-PS 282 para que el modo proxy continúe y complete el posicionamiento como se describe en X.S0024-0 3GPP2. Los mensajes POS SUPL pueden llevar mensajes IS-801 incorporados. El posicionamiento proporciona una estimación de posición para el UE 110, que se pasa al E-PS 282.

[118] En la etapa 12, el E-PS 282 selecciona un PSAP (por ejemplo, el PSAP 180) y obtiene un ESRD y un ESRK si el PSAP 180 admite PSTN. En la etapa 13, el E-PS 282 devuelve a la E-CSCF 254 una respuesta de encaminamiento que puede incluir una identidad del PSAP si el PSAP 180 admite IP, ESRD y ESRK si el PSAP 180 admite PSTN, y una estimación de posición para el UE 110 si es solicitada por la E-CSCF 254. El E-PS 282 puede almacenar para el UE 110 un registro de llamadas que contiene toda la información recopilada para el UE. Las etapas 14a y 15a se realizan si el PSAP 180 admite IP. Las etapas 14b, 14c y 15b se realizan si el PSAP 180 admite PSTN. En la etapa 16, después de establecida la llamada, el PSAP 180 puede enviar una solicitud de ubicación para una estimación de posición precisa al E-PS 282, que puede identificarse por una dirección IP o nombre obtenido en la etapa 14a o un ESRK obtenido en la etapa 14c.

[119] En la etapa 17, el E-PS 282 puede abrir una nueva transacción X.S0024 con el UE 110 enviando un SUPL INIT directamente al UE 110 usando una IP con terminación móvil o UDP/IP (en cuyo caso se omite la etapa 18) o enviando a la E-CSCF 254 un mensaje inmediato que contiene un SUPL INIT X.S0024 con los parámetros descritos en la etapa 7 excepto por una precisión/retardo de QoP para una estimación precisa de la posición. En la etapa 18, la E-CSCF 254 transfiere el SUPL INIT dentro de un mensaje IMS inmediato, un mensaje SIP o algún otro mensaje al UE 110. En la etapa 19, el UE 110 establece una conexión IP (por ejemplo, una conexión de IP segura) al E-PS 282 y devuelve un SUPL INICIO al E-PS 282. El E-PS 282 determina una PDE o un V-PS adecuado para el posicionamiento basándose en cualquier información de ubicación en el SUPL INICIO y en cualquier otra información de ubicación para el UE 110. El E-PS 282 luego comienza el posicionamiento devolviendo una SUPL RESPUESTA al UE 110. El UE 110 puede entonces intercambiar mensajes de POS SUPL con el E-PS 282, una PDE local, y/o una PDE remota para realizar el posicionamiento y obtener una estimación de posición precisa para el UE 110. En la etapa 20, el E-PS 282 envía la estimación precisa de la posición para el UE 110 en una Respuesta de Ubicación al PSAP 180.

[120] El UE 110 puede comunicarse después con el PSAP 180 para la llamada de VoIP de emergencia. Cuando la llamada se libera más tarde, la E-CSCF 254 puede enviar una indicación al E-PS 282, que luego puede liberar cualquier registro de la llamada. La E-CSCF 254 o el UE 110 también pueden anular el registro del ID de usuario público de emergencia, que se registró en las etapas 2 a 4. De forma alternativa, la E-CSCF 254, el E-PS 282 y el UE 110 pueden permitir que el registro y los registros de llamadas persistan durante un cierto período de tiempo para admitir una posible devolución de llamada posterior desde el PSAP 180 al UE 110 y/o solicitudes de ubicación adicionales.

[121] Detalles adicionales para las etapas 1 a 8 y las etapas 12 a 20 de la FIG. 9 pueden describirse para las etapas 1 a 8 y las etapas 12 a 20, respectivamente, de la FIG. 5.

[122] El flujo de mensajes 500 tiene las siguientes características relacionadas con X.S0024.

(a) Adición de una dirección del E-PS en un INIT SUPL X.S0024, que anula y reemplaza una dirección del H-PS configurada en el UE 110 o el UIM.

(b) Interfaz entre el lado del IMS (por ejemplo, la E-CSCF 254) y el lado de la ubicación (por ejemplo, el E-PS 282).

(c) Uso del V-PS 284 y descubrimiento de la dirección del V-PS.

(d) Transmisión de un INIT SUPL X.S0024 usando IP con terminación móvil, UDP/IP, señalización SIP o señalización IMS.

(e) Adición de una indicación de servicios de emergencia en el INIT SUPL X.S0024.

(f) Uso de un nuevo protocolo entre la E-CSCF 254 y el E-PS 282, que puede ser similar al protocolo OMA RLP o PS-PS en la interfaz LCS-z en X.S0024.

(g) Seguridad.

4. Admisión de UE sin UICC/UIM y/o acuerdo de itinerancia

[123] La descripción anterior supone que el UE 110 tiene una UICC o un UIM y que H-PLMN 160 y V-PLMN 130 tienen acuerdo de itinerancia, que permite el registro del UE en la V-PLMN 130 y el posterior acceso de llamada de emergencia al PSAP 180. Si este no es el caso, entonces el UE 110 puede acceder y registrarse en la V-PLMN 130 y puede completar la configuración de la llamada al PSAP 180 y la posible devolución de llamada desde el PSAP 180 como se describe a continuación. La devolución de llamada del PSAP 180 en el caso sin UICC/UIM es posible para VoIP, pero en general no es posible para el acceso de emergencia por conmutación de circuitos debido a la imposibilidad de ubicar un UE no registrado.

[124] **La FIG. 10** muestra un diagrama de bloques de un modo de realización de una arquitectura de red 1000 que admite la configuración de llamadas de VoIP de emergencia y la devolución de llamada del PSAP para un UE sin UICC/UIM. La arquitectura de red 1000 incluye algunas de las entidades mostradas en las FIGs. 2 y 3. La arquitectura de red 1000 también incluye un servidor de ubicación 286, que puede ser una SLP, un GMLC, un PS o alguna otra entidad de ubicación.

4.1. Acceso

[125] El UE 110 puede obtener acceso GPRS, acceso WLAN 3GPP o acceso IMS sin una UICC. El UE 110 también puede obtener acceso cdma2000, acceso WLAN 3GPP2 o acceso IMS sin un UIM. El UE 110 puede realizar diferentes procedimientos para diferentes tipos de acceso.

[126] Para el acceso GPRS, el UE 110 puede realizar la activación del contexto PDP para servicios de emergencia sin una UICC y/o sin un acuerdo de itinerancia en la V-PLMN 130 como se describe en TR 23.867 3GPP. La conexión de GPRS se puede lograr usando una pseudo IMSI, que puede registrar el UE 110 en el HSS 250 en la V-PLMN 130, que a su vez puede ayudar a dar soporte al traspaso entre SGSN. Si el UE 110 no tiene una UICC, entonces la pseudo IMSI se puede crear con una combinación única de MCC-MNC y dígitos de un IMEI. Si el UE 110 tiene una UICC pero no tiene acceso de itinerancia a V-PLMN 130, entonces la pseudo IMSI puede crearse con dígitos del IMSI en lugar del IMEI, lo que puede evitar el duplicado de pseudo IMSI si se usan todos los dígitos IMSI. La conexión GPRS también se puede lograr utilizando el IMEI como identificación.

[127] Para el acceso WLAN 3GPP, el UE 110 puede crear una pseudo NAI a partir de una pseudo IMSI (por ejemplo, la misma pseudo IMSI utilizada para la conexión GPRS), de la siguiente manera:

PseudoNAI = “n<pseudo IMSI>@V-PLMN_network_domain”

donde n es un dígito fijo en el intervalo de 2 a 9 que indica el uso de una pseudo NAI no autenticable para una llamada de emergencia (ya se han tomado 0 o 1 para NAI normales). El UE 110 puede usar el pseudo NAI para el acceso inicial y el procedimiento AAA.

[128] La WLAN puede anunciar V-PLMN capaces de admitir AAA usando el pseudo NAI para servicios de emergencia o puede presentar las V-PLMN en un orden priorizado que indique la capacidad y la disposición para respaldar esto. La V-PLMN 130 puede tratar al UE 110 como un abonado doméstico temporal y puede omitir AAA o asegurarse de que tenga éxito (por ejemplo, utilizando claves bien conocidas para asegurar que la autenticación tenga éxito). Puede ser deseable seguir los procedimientos normales en la medida de lo posible y registrar el UE 110 en HSS 250 para dar mejor soporte a la reselección y el traspaso WLAN.

[129] Para el acceso cdma2000, el UE 110 puede establecer una sesión PPP con el PDSN 242 y puede rechazar la autenticación durante el establecimiento PPP devolviendo un Configurar Rechazo de Protocolo de Control de Enlace (LCP) en respuesta a una Solicitud de Configuración LCP del PDSN 242, por ejemplo, como se describe en IETF RFC 1661. El PDSN 242 puede admitir llamadas de emergencia para UE sin UIM o no autenticados y puede continuar el establecimiento de sesión PPP sin autenticar el UE 110. El PDSN 242 puede asignar una dirección IP simple al UE 110 y puede aplicar un filtrado de paquetes IP para restringir las entidades con las que el UE 110 puede comunicarse. Por ejemplo, el PDSN 242 puede restringir el UE 110 a la comunicación con servidores locales (por ejemplo, un servidor DHCP, un servidor DNS y la P-CSCF 252) y con entidades asociadas con el acceso PSAP pero no con acceso abierto a Internet.

[130] El PDSN 242 puede ser informado de una llamada de emergencia de varias maneras. En un modo de realización, el UE 110 envía al PDSN 242 una solicitud de configuración IPCP que contiene una dirección IP única que se define globalmente para indicar una solicitud de dirección IP para una llamada de emergencia. En otros modos de realización, las indicaciones pueden usarse en el establecimiento de PPP, o el PDSN 242 puede recibir una indicación de una solicitud de llamada de emergencia desde la RAN (RRC/PCF 222) a través de la interfaz cdma2000 A10. En cualquier caso, el PDSN 242 puede asignar una dirección IP simple a un UE no autenticado para una llamada de emergencia y puede emplear un filtrado especial como se describió anteriormente. Esta asignación de dirección IP se puede lograr a través de una mejora en el IPCP PPP descrita en IETF RFC 1332. Si el UE 110 no indica una llamada de emergencia, entonces el PDSN 242 puede rechazar el establecimiento de PPP y la asignación de la dirección IP.

[131] En lugar de rechazar la autenticación, el UE 110 puede permitir que la autenticación proceda usando un protocolo de autenticación de contraseña (PAP) o un protocolo de autenticación por desafío de reto (CHAP), que se describen en IETF RFC 1334 y RFC 1994, respectivamente. El UE 110 puede recibir un desafío CHAP o una solicitud de autenticación PAP y puede enviar una respuesta que incluye una identidad que indica una llamada de emergencia desde un UE sin UIM. Esta identidad puede ser la pseudo IMSI usada para el acceso WLAN 3GPP2. Si la identidad indicaba V-PLMN 130 como el dominio para el UE 110, entonces la autenticación CHAP o PAP puede proceder de la manera habitual desde la perspectiva del PDSN 242 al servidor AAA 246 en la V-PLMN 130. El servidor AAA 246 puede reconocer la pseudo IMSI como indicación de acceso de llamada de emergencia y puede renunciar a la autenticación normal o puede realizar la autenticación utilizando claves conocidas. El servidor AAA 246 puede asegurar que el PDSN 242 usa el filtrado restringido para restringir el acceso de IP, por ejemplo, para permitir una llamada de VoIP de emergencia pero no otros tipos de acceso.

[132] El PDSN 242 puede construir una NAI para contabilidad y/o mantenimiento de registros. El PDSN 242 puede usar la identidad internacional única del UE (una IMSI, MIN o itinerancia internacional MIN - IRM) si el UE 110 tiene un UIM. El PDSN 242 también puede usar un ESN u otra identificación para el UE 110.

[133] Para el acceso WLAN 3GPP2, después de que el UE 110 acceda a la WLAN, un punto de acceso o una entidad de autenticación puede iniciar la autenticación del UE 110 y puede enviar una solicitud de protocolo de autenticación extensible (EAP) o alguna otra solicitud de identidad del UE 110. El UE 110 puede responder devolviendo una respuesta EAP o alguna otra respuesta que contenga la identidad del UE, por ejemplo, en la forma de usuario@dominio donde el dominio identifica la H-PLMN del UE 110. Si el UE 110 no tiene UIM o no hay acuerdo de itinerancia en la V-PLMN 130, entonces el UE 110 puede devolver una pseudoidentidad que puede ser la misma, o similar a, la pseudo NAI usada para la WLAN 3GPP. Por ejemplo, la parte del usuario (por ejemplo, la pseudo IMSI) de la pseudoidentidad puede contener dígitos de la identidad internacional única del UE (por ejemplo, IMSI, MIN o IRM) si el UE 110 tiene un UIM o, de otro modo, dígitos del ID del terminal único (por ejemplo, un ESN). La porción de usuario también puede contener un prefijo único (por ejemplo, un dígito único) para indicar que se trata de una pseudoidentidad para llamadas de emergencia. La porción de dominio de la pseudoidentidad puede indicar la V-PLMN 130.

[134] El punto de acceso o entidad de autenticación puede continuar la autenticación usando un servidor AAA local, por ejemplo, el servidor AAA 246. La autenticación puede ejecutarse normalmente usando claves conocidas o puede truncarse debido a que la autenticación genuina no tiene lugar. Una vez que se completa la pseudoautenticación, el punto de acceso o el encaminador asociado puede emplear el filtrado de paquetes para limitar el acceso del UE 110, como se describió anteriormente.

[135] El UE 110 puede acceder a la WLAN, realizar pseudautenticación y descubrir una PDIF. El UE 110 puede entonces identificarse con la PDIF (o el servidor AAA local) usando una pseudoidentidad, por ejemplo, en lugar de una NAI usada para la autenticación UE-PIDF de cdma2000. La pseudoidentidad puede ser la misma o similar a la utilizada para la autenticación WLAN. La autenticación normal y el establecimiento del túnel pueden entonces proceder (por ejemplo, como se describe en X.P0028-200 3GPP2) usando el servidor local AAA y empleando claves conocidas para lograr cierta transparencia para la PDIF. De forma alternativa, la autenticación puede ser truncada o cancelada. Después de la autenticación, la PDIF puede emplear el filtrado de paquetes para limitar el acceso del UE 110.

[136] La WLAN puede anunciar V-PLMN capaces de admitir los procedimientos anteriores o puede presentar las V-PLMN en un orden priorizado que indique la capacidad y la disposición para admitir esto.

[137] Para el acceso IMS, el registro SIP puede omitirse si el UE 110 no tiene UICC/UIM y/o no hay acuerdo de itinerancia en la V-PLMN 130, como se describe en TR 23.867 3GPP y X.P0013-002A 3GPP2. Esto permite la configuración de llamadas de emergencia a un PSAP, pero no admite la devolución de llamadas. De forma alternativa, el UE 110 puede registrarse enviando un SIP REGISTRAR que contiene un nombre de dominio de la V-PLMN y un ID de usuario privado de emergencia, que se puede crear usando el nombre de dominio de la V-PLMN y una pseudo IMSI. Este SIP REGISTRAR se reconocería en la E-CSCF 254 y el HSS 250, pero podría ser transparente para otras entidades.

[138] El procedimiento de registro puede entonces proceder hasta la transmisión del SIP REGISTRAR desde el UE 110 a la E-CSCF 254 (u otro servidor IMS) en la V-PLMN 130. El registro en la H-PLMN 160 no se realiza, pero la E-CSCF 254 registraría el UE 110 en el HSS 250 en la V-PLMN 130. El HSS 250 puede asignar un URI del TEL temporal y/o un URI de SIP temporal (de un grupo de HSS 250) como identidades de usuario públicas temporales. El URI del TEL puede transmitirse al PSAP 180 en la configuración de la llamada si la señalización se realizó a través de la PSTN, y el URI del SIP puede transmitirse para la configuración de la llamada SIP. El URI habilitaría la devolución de llamada desde el PSAP 180 si tanto la V-PLMN 130 como el UE 110 mantienen el registro IMS y la conectividad IP durante algún tiempo después de la finalización de la llamada de emergencia. El URI del TEL y el URI de SIP son reconocidos por el PSAP 180 como direcciones temporales debido a las diferencias de las direcciones permanentes normales, ya que no se usan para identificar globalmente al UE 110. El HSS 250 puede "poner en cuarentena" las direcciones temporales devueltas de las llamadas de emergencia finalizadas y no reasignar estas direcciones durante un período de tiempo para evitar que las devoluciones de llamada del PSAP se desvíen a UE incorrectos.

[139] La devolución de llamada del PSAP puede ser compatible de varias maneras. Si el UE 110 está registrado en la H-PLMN 160, la devolución de llamada desde el PSAP 180 puede usar la identidad de usuario pública URI de SIP o URI del TEL del UE 110 y puede encaminarse inicialmente a la H-PLMN 160, como se describe en TS 23.228 de 3GPP o X.P0013 de 3GPP2. Para un PSAP compatible con SIP, el SIP INVITAR puede encaminarse a la I-CSCF 262 en la H-PLMN 160 (basándose en el nombre de dominio de la H-PLMN en el URI de SIP del UE). La I-CSCF 262 puede consultar el HSS 250 para la S-CSCF 264 en la H-PLMN 160 y luego puede encaminar la llamada a la S-CSCF 264. La S-CSCF 264 puede entonces encaminar la llamada a la E-CSCF 254 o la P-CSCF 252 en la V-PLMN 130 basándose en la anterior información de registro. En el primer caso, la E-CSCF 254 puede tratarse mediante la S-CSCF 264 como una P-CSCF y puede encaminar la llamada a través de la P-CSCF 252 al UE 110. En este último caso, la P-CSCF 252 puede encaminar la llamada al UE 110. Para un PSAP compatible con PSTN, la llamada puede encaminarse a través de la PSTN a una MGCF en la H-PLMN 160 basándose en el URI de TEL del UE 110. La MGCF puede interfuncionar entre la señalización SIP y PSTN y puede enviar un SIP INVITAR a la I-CSCF 262 en la H-PLMN 160. El encaminamiento de llamadas de I-CSCF 262 al UE 110 procedería entonces de la misma manera que para un PSAP compatible con SIP.

[140] Si el UE 110 no está registrado en la H-PLMN 160 (por ejemplo, debido a que no hay UICC/UIM y/o no hay acuerdo de itinerancia con la V-PLMN 130), entonces el UE 110 puede registrarse en el HSS 250 en la V-PLMN 130. El HSS 250 puede asignar una identidad de usuario pública URI de TEL o URI de SIP temporal al UE 110. La devolución de llamada desde el PSAP puede encaminarse a la I-CSCF 256 para un PSAP compatible con SIP o MGCF 258 para un PSAP compatible con PSTN, sin involucrar a la H-PLMN 160.

4.2. <u>Configuración de llamada</u>

[141] **La FIG. 11** muestra un modo de realización de un flujo de mensajes 1100 para la configuración de llamadas de VoIP de emergencia para un UE sin UICC/UIM. El flujo de mensajes 1100 se puede usar para la ubicación del plano de control 3GPP, SUPL y X.S0024.

[142] En la etapa 1, el UE 110 descubre y se conecta a una red de acceso, establece conectividad IP y puede descubrir un servidor SIP local (por ejemplo, la P-CSCF 252), como se describió anteriormente. El UE 110 puede emplear una pseudo IMSI para el acceso cdma2000 o GPRS, una pseudo NAI para acceso WLAN, una pseudoidentidad para el acceso WLAN 3GPP2. El UE 110 puede registrarse en el HSS 250 en la V-PLMN 130 usando la pseudoidentidad (por ejemplo, una pseudo IMSI).

[143] En la etapa 2, el UE 110 intenta registrarse en la red V-PLMN IMS enviando un SIP REGISTRAR a la P-CSCF 252, que se descubrió en la etapa 1. Sin UICC/UIM o sin itinerancia, el SIP REGISTRAR puede incluir una indicación de servicios de emergencia, el nombre de dominio de V-PLMN, la dirección IP del UE obtenida en la etapa 1, un ID de usuario privado de emergencia creada utilizando el nombre de dominio de V-PLMN y la pseudo IMSI (para GPRS) o pseudoidentidad (para cdma2000) y/u otra información. Para volver a registrarse, el SIP REGISTRAR puede incluir, además, un ID de usuario público temporal asignada en el registro inicial. Debido a la presencia de la indicación de servicios de emergencia o al ID de usuario privado de emergencia (que puede indicar la V-PLMN 130 como la red doméstica para el UE 110), la P-CSCF 252 envía el SIP REGISTRAR a la E-CSCF 254, que admite llamadas de servicio de emergencia, en la misma red. El SIP REGISTRAR reenviado puede incluir información de ubicación para el UE 110. El SIP REGISTRAR también puede incluir una dirección V-SLP o SGSN (para 3GPP) o una dirección V-SLP, PDSN o PIDF (para 3GPP2).

[144] En la etapa 3, debido a que el ID de usuario privado de emergencia para el UE 110 hace referencia a la V-PLMN 130, la E-CSCF 254 reenvía la información de registro al HSS 250, por ejemplo, en un Cx-Put/Cx-Pull. En la etapa 4, el HSS 250 verifica si el ID de usuario privado de emergencia ya está registrado, por ejemplo, si el UE 110 ya está registrado u otro UE registrado con el mismo ID de usuario privado. El HSS 250 puede usar el ID de usuario público temporal, si se proporciona, para distinguir los UE que tienen el mismo ID de usuario privado de emergencia debido a los dígitos comunes de entidad del UE (por ejemplo, dígitos comunes de IMEI o ESN) y para distinguir un registro inicial (sin usuario público temporal asignado) desde un nuevo registro. Para un

registro inicial, el HSS 250 almacena el ID de usuario privado de emergencia y la dirección E-CSCF y asigna un URI de SIP y/o un URI de TEL de usuario público temporal, que se devuelven a E-CSCF 254.

[145] En la etapa 5, E-CSCF 254 devuelve un 200 OK al UE 110 a través de P-CSCF 252. El 200 OK puede incluir los ID de usuario públicos temporales asignados por HSS 250. El UE 110 puede volver a registrarse si se transfiere a una SGSN diferente (para acceso GPRS), una PCF o PDSN diferente (para acceso cdma2000), una WLAN diferente (para acceso WLAN) dentro de V-PLMN 130. En la etapa 6, el UE 110 envía a P-CSCF 252 un SIP INVITAR que puede incluir un URL de SIP o URI del TEL global que indica una llamada de emergencia, el tipo de servicio de emergencia necesario, y los ID de usuario públicos temporales recibidos en la etapa 5 si el UE 110 no tiene UICC/UIM y/o no tiene acceso de itinerancia a la V-PLMN 130. P-CSCF 252 envía el SIP INVITAR a E-CSCF 254. En la etapa 7, E-CSCF 254 interactúa con el servidor de ubicación 286 para obtener información de encaminamiento PSAP para la llamada (por ejemplo, URI de SIP del PSAP, o ESRD y ESRK), como se describe para las etapas 6 a 13 de las FIGs. 5 y 9 y las etapas 9 a 13 de la FIG. 7.

[146] Las etapas 8a y 9a se realizan si el PSAP 180 admite IP. En la etapa 8a, E-CSCF 254 encamina el SIP INVITAR al PSAP 180 usando un URI de SIP. El SIP INVITAR puede incluir cualquier estimación de posición provisional para el UE 110, la dirección IP o el nombre del servidor de ubicación 286, y el URI de SIP del usuario público temporal asignado al UE 110. En la etapa 9a, se puede intercambiar la señalización SIP adicional para establecer la llamada de emergencia.

[147] Las etapas 8b, 8c y 9b se realizan si el PSAP 180 admite PSTN. En la etapa 8b, E-CSCF 254 envía el SIP INVITAR a través de una BGCF a MGCF 258. El SIP INVITAR puede incluir el ESRD y ESRK y posiblemente un URI de TEL público de usuario temporal asignado al UE 110. En la etapa 8c, la MGCF 258 encamina la llamada al PSAP 180 a través de la PSTN, posiblemente a través de un encaminador selectivo, usando SS7 ISUP y/o señalización MF. El ESRD o ESRK se usan como números de encaminamiento y el ESRK se pasa a PSAP 180 como la identidad del UE 110 y como una clave para obtener más información. También se puede pasar un número de usuario E.164 público temporal al PSAP 180 si lo permiten las capacidades de señalización. E.164 es una norma ITU-T que define el sistema de numeración telefónica internacional, y un número E.164 se compone de un código de país más un número nacional. En la etapa 9b, puede intercambiarse la señalización SIP adicional y puede producirse interfuncionamiento con SS7 ISUP y/o MF en la MGCF 258 para establecer la llamada.

[148] En la etapa 10, el PSAP 180 puede obtener una estimación precisa de la posición para el UE 110 consultando el servidor de ubicación 286, que puede indicarse mediante el URI de SIP o ESRK en la configuración de la llamada. La respuesta del servidor de ubicación 286 puede incluir cualquier número de usuario público temporal E.164 asignado al UE 110, si el PSAP 180 admite PSTN y si este número no se pasó al PSAP 180 en la configuración de la llamada. La llamada puede ser liberada un tiempo después, por ejemplo, interrumpirse debido a la pérdida temporal de la cobertura de radio. La E-CSCF 254 puede entonces esperar durante un período de tiempo antes de informar al servidor de ubicación 286 para dar soporte a la ubicación del UE 110 por el PSAP 180 para una posterior devolución de llamada.

[149] El PSAP 180 intenta devolver la llamada al UE 110 utilizando su ID de usuario público temporal. La etapa 11a se realiza para un PSAP compatible con SIP. En la etapa 11a, el PSAP 180 envía un SIP INVITAR a I-CSCF 258, que puede indicarse mediante la parte de dominio de red del URI de SIP de usuario público temporal asignado al UE 110. Las etapas 11b y 11c se realizan para un PSAP compatible con PSTN. En la etapa 11b, el PSAP 180 envía una ISUP IAM (o configuración de llamada MF) a MGCF 258, que puede indicarse mediante los primeros dígitos del número de usuario público temporal E.164 asignado al UE 110. En la etapa 11c, la MGCF 258 envía a I-CSCF 258 un SIP INVITAR que contiene un URI de TEL construido a partir del número E.164 recibido en la etapa 11b.

[150] En la etapa 12, I-CSCF 258 envía al HSS 250 una consulta de ubicación que puede incluir el URI de SIP de usuario público temporal recibido en la etapa 11a o el URI de TEL de usuario público temporal recibido en la etapa 11c. En la etapa 13, HSS 250 encuentra la información de registro del UE y devuelve la dirección de E-CSCF 254 a I-CSCF 258. En la etapa 14, I-CSCF 258 envía el SIP INVITAR al E-CSCF 254. En la etapa 15, la E-CSCF 254 ubica la dirección P-CSCF y envía el SIP INVITAR a través de P-CSCF 252 al UE 110. En la etapa 16, la configuración de la llamada continúa como en un caso normal.

[151] El UE 110 puede comunicarse después con el PSAP 180. Cuando se libera la llamada o algún tiempo después, la E-CSCF 254 puede enviar una indicación al servidor de ubicación 286, que luego puede liberar cualquier registro de la llamada.

5. <u>Admisión de PSAP heredado geográficamente remoto</u>

[152] En algunos casos, el servidor de V-PLMN y/o SIP (por ejemplo, E-CSCF 254) puede estar geográficamente alejado del UE 110. En dichos casos, puede que no sea posible encaminar la llamada a través

de una MGCF local a un PSAP compatible con PSTN si la PSTN no admite el acceso a PSAP remotos. Lo siguiente puede usarse para abordar estos casos.

[153] En un modo de realización, la llamada de emergencia se redirige a una V-PLMN diferente. Al principio del procesamiento de SIP INVITAR, una E-CSCF o un servidor de ubicación (por ejemplo, una E-SLP, un GMLC, etc.) pueden determinar que la llamada debe redirigirse a un servidor de llamadas en otra red. En ese caso, una respuesta redirección SIP 3xx (por ejemplo, proxy de uso 305) que contiene el URI de SIP del servidor o servidores alternativos preferidos puede devolverse al UE 110. El UE 110 puede entonces volver a intentar los procedimientos de llamada como se describió anteriormente, aunque los procedimientos de acceso y conectividad IP pueden omitirse si todavía se puede usar la misma red de acceso. Si el procedimiento de configuración de llamada ha avanzado tanto como para determinar una estimación de posición provisional y/o el PSAP correcto (por ejemplo, ESRD, URI de SIP o dirección de IP), entonces la E-CSCF puede incluir estos en la respuesta de redirección. El UE 110 puede incluir entonces la información en el SIP INVITAR enviado a la nueva PLMN, que puede evitar un retardo adicional para obtener la misma información y permitir el uso de la PLMN sin la capacidad de obtener esta información. La E-CSCF original puede notificar al servidor de ubicación (por ejemplo, E-SLP o GMLC), que luego puede eliminar el registro de llamadas para el UE 110.

[154] En otro modo de realización, la E-CSCF reenvía la llamada a un servidor SIP en otra red (o la misma red) más cerca de un PSAP desde el que la llamada puede reenviarse mejor a la PSTN. La V-PLMN puede seguir admitiendo todas las funciones descritas anteriormente, incluidas las funciones de ubicación y admitir UE sin UICC o UIM. El SIP INVITAR reenviado puede incluir la identidad del PSAP (por ejemplo, URI de SIP o ESRD), cualquier ESRK asignado por el servidor de ubicación y cualquier ID de usuario público temporal asignada para un UE sin UICC. El PSAP puede continuar consultando el servidor de ubicación en la V-PLMN para obtener información de ubicación y cualquier devolución de llamada puede enviarse a través de la H-PLMN a la V-PLMN para el caso normal o dirigirse a la V-PLMN en el caso sin UICC. La admisión continua de estas funciones en la V-PLMN evita las demandas en el servidor SIP posterior y debe permitir que un mayor número de otras redes admita el servicio de reenvío.

[155] En otro modo de realización más, se puede usar la Portabilidad del Número Local, por ejemplo, en América del Norte. Además de devolver el ESRD y ESRK, el servidor de ubicación (por ejemplo, E-SLP o GMLC) puede devolver un LRN (Número de encaminamiento de ubicación) a la red IMS (por ejemplo, E-CSCF) que corresponde a un intercambio LEC o un encaminador selectivo PSAP desde el cual se puede llegar al PSAP directamente. Como alternativa, la red IMS (por ejemplo, E-CSCF o MGCF) puede obtener el LRN del ESRD. El LRN está incluido en la información enviada a la MGCF (si no es obtenido por la MGCF), y la MGCF envía a la PSTN un ISUP IAM que contiene los siguientes parámetros:

Número de la parte llamada = LRN,
Parámetro genérico de dirección (GAP) = ESRD,
El bit M del parámetro FCI configurado como "número traducido",
Número de la parte que llama = UE MSISDN o ESRK, y
La categoría de la parte que llama se establece en "llamada de servicio de emergencia" (opcional).

[156] Debido a admitir la portabilidad numérica por las PSTN (por ejemplo, a lo largo de los EE. UU.), la llamada (ISUP IAM) puede encaminarse correctamente al LEC CO o encaminador selectivo siempre que se pueda usar SS7 en lugar de MF troncales. El encaminador selectivo o LEC CO de destino puede admitir la portabilidad numérica y puede reconocer el LRN como propio al recibir la llamada y puede obtener el verdadero número de la parte llamada (el ESRD) del GAP. La singularidad del ESRD o la configuración de categoría de la parte que llama puede informar al LEC CO o al encaminador selectivo que se trata de una llamada de emergencia. En ese punto, la llamada puede encaminarse al PSAP como si se hubiera originado localmente. Este modo de realización evita nuevos impactos a los conmutadores interurbanos de la PSTN (por ejemplo, sin cambios de encaminamiento) pero puede afectar los LEC CO y los encaminadores selectivos.

6. <u>Seguridad para SUPL y X.S0024</u>

[157] Para SUPL, se pueden establecer procedimientos de seguridad para admitir la E-SLP 272 reemplazando a la H-SLP para el posicionamiento tanto en escenarios de itinerancia como no itinerantes y con modo proxy o no proxy. Los procedimientos de seguridad SUPL existentes se basan, en general, en claves compartidas tanto en el UE 110 como en la H-SLP y/o en otra información proporcionada en el UE 110 con respecto a la H-SLP (por ejemplo, nombre de dominio completo, certificado de clave pública raíz X.509, etc.). Dicha información puede no estar disponible para E-SLP 272. Para E-SLP 272, la autenticación para los modos proxy y no proxy se puede admitir como se describe a continuación.

[158] Para X.S0024, también se pueden establecer procedimientos de seguridad para admitir E-PS 282 reemplazando el H-PS para posicionamiento. Los procedimientos de seguridad X.S0024 existentes se describen en X.S0024-0 de 3GPP2 y en S.P0110-0 de 3GPP2. Estos procedimientos usan una clave de raíz común

proporcionada tanto en el H-PS para un usuario como en el UIM del usuario. Las claves adicionales se pueden obtener de la clave raíz proporcionada de la siguiente manera:

(a) Clave para admitir almacenamiento seguro y encapsulación directa (S-SAFE) en el que se envía un SUPL INIT al UE 110 usando SMS o WAP Push y se autentica (como procedente del H-PS) y se cifra opcionalmente.

(b) Clave para admitir una conexión IP segura entre el UE 110 y el H-PS en el que los mensajes X.S0024 se envían entre el UE 110 y el H-PS con cifrado y autenticación.

(c) Clave para admitir una conexión IP segura entre el UE 110 y una PDE para el modo no proxy en el que los mensajes X.S0024 se envían entre el UE 110 y la PDE con cifrado y autenticación.

[159] Cada una de las tres claves descritas anteriormente se corrige en el sentido de que hay un valor determinista para cualquier valor de la clave raíz. Sin embargo, a partir de cada una de estas claves fijas, pueden obtenerse claves adicionales para el cifrado y la autenticación cuyos valores dependen de números aleatorios proporcionados para una sesión de posicionamiento particular por el UE y el H-PS o la PDE. Esta obtención de clave y los procedimientos de seguridad acompañantes hacen uso del procedimiento de seguridad de la capa de transporte (TLS) descrito en IETF RFC 2246 y su variante PSK-TLS descrita en el borrador del IETF "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)" ["Series criptográficas de clave precompartida para seguridad de la capa de transporte (TLS)"]. Si X.S0024 se usa para el posicionamiento en una llamada de VoIP de emergencia y el E-PS 282 no es el H-PS, entonces ya no es posible confiar en una clave raíz preconfigurada común en ambos UE 110 y E-PS 282 para la autenticación mutua y cifrado.

[160] Para SUPL, el UE 110 puede autenticar la E-SLP 272 para evitar el acceso no autorizado a la ubicación del UE incluso durante una llamada de emergencia. Para X.S0024, el UE 110 y la E-PS 282 pueden realizar la autenticación mutua. La Tabla 2 enumera cinco procedimientos de autenticación, designados como procedimientos A, B, C, D y E, y las características de cada procedimiento.

Tabla 2 - Procedimientos de autenticación

Característica	**Procedimiento A**	**Procedimiento B**	**Procedimiento C**	**Procedimiento D**	**Procedimiento E**
Autenticar E-SLP	No	Sí	Sí	Sí	Sí
Autentica UE	No	Limitado	Sí	Sí	Sí
Admite itinerancia	Sí	Sí	Sí	Sí	No
Impacto en H-PLMN	No	No	No	Sí	Sí
Conexión segura del UE al IMS necesaria	No	No	Sí	No	No
Admite sin UICC/UIM	Sí	Sí (nota 1)	Limitado	No	No
Nota 1: se supone que los certificados raíz de clave pública se proporcionan en un equipo móvil (ME)					

[161] El procedimiento A proporciona una autenticación mínima. El UE 110 permite la ubicación SUPL o X.S0024 iniciada por la red desde una E-SLP o un E-PS no autenticado si el mensaje SUPL INIT indica la ubicación para una sesión de emergencia y el UE 110 está actualmente ocupado en una sesión de emergencia. La restricción a la sesión de emergencia proporciona cierta protección. Para SUPL, el UE 110 puede seleccionar el procedimiento A al no invocar procedimientos de seguridad con E-SLP 272. En este caso, E-SLP 272 aún puede verificar la identidad del UE, en una extensión limitada, a través de un código hash INIT SUPL contenido en un POS INIT SUPL. Además, la dirección IP del UE 110 proporcionada a E-SLP 272 por E-CSCF 254 puede proporcionar alguna seguridad adicional de la identidad correcta del UE. Para X.S0024 y SUPL, la transferencia de SUPL INIT a través del IMS o SIP (si no se utiliza la transferencia directa a través de IP con terminación móvil o UDP/IP) puede brindar cierta confianza adicional en la autenticidad del UE, ya que la transferencia IMS y SIP depende de la admisión y verificación de V-PLMN 130 y/o H-PLMN 160.

[162] El procedimiento B es para autenticación de clave pública TLS. UE 110 y E-SLP 272 o E-PS 282 admiten la autenticación de clave pública usando TLS como se describe en IETF RFC 2246 y también describen un mecanismo de autenticación de cliente alternativo en OMA SUPL 1.0, "Secure User Plane Location Architecture" ["Arquitectura de ubicación de plano de usuario seguro"]. Este mecanismo admite la autenticación de la H-SLP o el E-PS por un UE que usa TLS con certificados de clave pública ITU X.509 enviados por la H-SLP o el E-PS al UE durante una fase de establecimiento de enlace TLS. Los certificados de clave pública proporcionan una cadena de firmas digitales, autenticando cada firma la siguiente, de modo que el UE puede

autenticar la clave pública de la E-SLP o el E-PS siempre que el UE esté provisto de la clave pública de al menos una autoridad de certificación raíz. El procedimiento TLS de autenticación de clave pública admite la transferencia de claves simétricas para su uso en el posterior cifrado y autenticación de la señalización, por ejemplo, para mensajes SUPL posteriores. La autenticación y el cifrado entre el UE 110 y un SPC o PDE para el modo no proxy también pueden ser admitidos con estas claves u obteniendo claves adicionales de estas claves. El procedimiento B se basa en la certificación de la clave o claves públicas de E-SLP o E-PS por una o más autoridades de certificación raíz (por ejemplo, definida por OMA) y la dotación de la clave o claves en los UE que admiten SUPL o X.S0024 para llamadas de VoIP de emergencia. Esto asegura la autenticación de E-SLP 272 o E-PS 282 por el UE 110 y, para SUPL, la autenticación limitada del UE 110 por E-SLP 272 a través de un código hash INIT SUPL de 64 bits incluido en POS INIT SUPL y enviado por el UE 110 a E-SLP 272.

[163] Para el procedimiento B, el UE 110 (por ejemplo, con UICC o UIM) puede dotarse de uno o más certificados de clave pública raíz que permiten al UE verificar la clave o claves públicas de E-SLP 272 o E-PS 282. El UE 110 y la E-SLP 272 o el E-PS 282 pueden establecer una clave de cifrado compartida y una clave de código de autenticación de mensaje (MAC) usando procedimientos TLS descritos en RFC 2246 y uno o más procedimientos seguros de transferencia de clave pública, por ejemplo, RSA, DSS o Diffie-Hellman. El cifrado y la autenticación de los mensajes SUPL o X.S0024 se pueden realizar después del establecimiento de una conexión TLS segura. Para el modo no proxy, el procedimiento definido para el modo no proxy 3GPP2 en SUPL 1.0 se puede usar para generar una clave compartida para la autenticación y el cifrado, de acuerdo con IETF PSK-TLS, entre el UE 110 y un V-SPC o H-SPC en SUPL o entre el UE 110 y una PDE en X.S0024.

[164] El procedimiento C es para la autenticación PSK-TLS. El UE 110 y la E-SLP 272 o el E-PS 282 admiten PSK-TLS (por ejemplo, como se describe en SUPL 1.0 para SET 3GPP2 o X.S0024-0 y S.P0110-0 3GPP2) de acuerdo con el borrador del IETF "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)" ["Series criptográficas de clave precompartida para seguridad de la capa de transporte (TLS)"]. Una clave precompartida (PSK) puede generarse a partir de (a) información (por ejemplo, información aleatoria) aportada por el UE 110, la red IMS (por ejemplo, E-CSCF 254) y/o E-SLP 272 o E-PS 282 (b) información (por ejemplo, parámetros SIP) enviada por o al UE 110 durante el establecimiento SIP de la llamada de emergencia, (c) información de seguridad ya presente en la P-CSCF 252 y el UE 110 para admitir el acceso seguro IMS desde el UE 110 (por ejemplo, usando IPsec, PSK-TLS, TLS), y/o (d) otra información. La información de seguridad en (c) puede estar disponible si el UE 110 se registra con la red H-PLMN IMS a través de V-PLMN 130.

[165] El PSK o la información usada para obtenerlo pueden estar disponibles para el UE 110 y la E-SLP 272 o el E-PS 282 durante el registro SIP y/o el inicio de una llamada de emergencia SIP y pueden usarse para la ubicación SUPL o X.S0024 usando PSK-TLS. La relación de confianza establecida durante el registro y la configuración de la llamada SIP entre estas entidades se usa para obtener una PSK segura o información común de la que se puede obtener una clave segura. Para SUPL, la autenticación mutua del UE 110 y la E-SLP 272 puede entonces admitirse usando PSK-TLS cuando el UE establece una conexión IP (PSK-TLS) a E-SLP 272 luego de la transferencia del SUPL INIT desde la E-SLP 272 al UE 110. Para X.S0024, la PSK segura se puede usar como una clave raíz de la cual se puede obtener la información de seguridad restante como se describe en X.S0024-0 y S.P0110-0 de 3GPP2.

[166] El procedimiento C se basa en una conexión segura entre el UE 110 y el IMS durante el registro SIP y/o la configuración de llamada SIP, lo que implica el registro del UE 110 en V-PLMN 130 y H-PLMN 160 y la autenticación mutua del UE 110 y V-PLMN 130. Si el UE 110 no tiene UICC/UIM o si no hay acuerdo de itinerancia entre V-PLMN 130 y H-PLMN 160, la autenticación mutua y la transmisión segura entre V-PLMN 130 y el UE 110 pueden no lograrse durante el registro SIP y la configuración de llamadas SIP y cualquier PSK generada proporcionarán una protección más limitada.

[167] El procedimiento D es para la autenticación con una arquitectura genérica de arranque (GBA) descrita en TS 33.220 de 3GPP o el borrador S.P0109 de TSG-S de 3GPP2. El UE 110 y la E-SLP 272 o el E-PS 282 admiten GBA. Esto permite que el UE 110 y la E-SLP 272 o el E-PS 282 obtengan una clave compartida segura de H-PLMN 160. Para SUPL, esta clave se puede usar para admitir la autenticación mutua PSK-TLS entre el UE 110 y la E-SLP 272, como se describe en TS 33.222 de 3GPP o el borrador S.P0114 de TSG-S de 3GPP2. Este procedimiento se utiliza en SUPL 1.0 para admitir el modo de proxy 3GPP. La clave también se puede usar para admitir TLS con autenticación HTTP Digest (por ejemplo, como se describe en TS 33.222 de 3GPP), solo autenticación HTTP Digest entre el UE 110 y la E-SLP 272 (por ejemplo, como se describe en el borrador S.P0114 de TSG-S de 3GPP2), u otras formas de autenticación. Para X.S0024, esta clave se puede usar como una clave raíz de la cual se puede obtener el resto de la información de seguridad.

[168] El procedimiento D se basa en admitir GBA en H-PLMN 160 así como también en V-PLMN 130 y un acuerdo de itinerancia entre V-PLMN 130 y H-PLMN 160 para permitir la transferencia de información clave desde una función de servicio de arranque (BSF) en H-PLMN 160 a una función de aplicación de red E-SLP (NAF) en V-PLMN 130.

[169] El procedimiento E es para la autenticación SUPL 1.0 o X.S0024. Para SUPL, si el UE 110 está en H-PLMN 160, entonces la E-SLP 272 puede ser la H-SLP, y se pueden usar los mecanismos de autenticación existentes definidos en SUPL 1.0. Para X.S0024, si el UE 110 está en H-PLMN 160, entonces el E-PS 282 puede ser el H-PS, y se pueden usar mecanismos de autenticación existentes definidos en X.S0024.

[170] **La FIG. 12** muestra un diagrama de bloques de un modo de realización del UE 110, la red de acceso 120, la E-CSCF 254 y el servidor de ubicación 286. El servidor de ubicación 286 puede ser E-SLP 272, GMLC 276, E-PS 282, y/o alguna otra entidad. Para simplificar, la FIG. 12 muestra solo un procesador 1210, una unidad de memoria 1212 y un transceptor 1214 para el UE 110, solo un procesador 1220, una unidad de memoria 1222, un transceptor 1224 y una unidad de comunicación (Comm) 1226 para la red de acceso 120, solo un procesador 1230, una unidad de memoria 1232 y una unidad de comunicación 1234 para E-CSCF 254, y solo un procesador 1240, una unidad de memoria 1242 y una unidad de comunicación 1244 para el servidor de ubicación 286. En general, cada entidad puede incluir cualquier cantidad de procesadores, unidades de memoria, transceptores, unidades de comunicación, controladores, etc.

[171] En el enlace descendente, las estaciones base y/o puntos de acceso en la red de acceso 120 transmiten datos de tráfico, señalización y piloto a los UE dentro de su área de cobertura. Estos diversos tipos de datos son procesados por el procesador 1220 y acondicionados por el transceptor 1224 para generar una señal de enlace descendente, que se transmite a través de una antena. En el UE 110, las señales de enlace descendente desde estaciones base y/o puntos de acceso se reciben a través de una antena, acondicionada por el transceptor 1214, y procesadas por el procesador 1210 para obtener diversos tipos de información para la ubicación, VoIP y otros servicios. Por ejemplo, el procesador 1210 puede descodificar mensajes usados para los flujos de mensajes descritos anteriormente. Las unidades de memoria 1212 y 1222 almacenan códigos de programa y datos para el UE 110 y la red de acceso 120, respectivamente. En el enlace ascendente, el UE 110 puede transmitir datos de tráfico, señalización y piloto a estaciones base y/o puntos de acceso en la red de acceso 120. Estos diversos tipos de datos son procesados por el procesador 1210 y acondicionados por el transceptor 1214 para generar una señal de enlace ascendente, que se transmite a través de la antena del UE. En la red de acceso 120, las señales de enlace ascendente del UE 110 y otros UE son recibidas y acondicionadas por el transceptor 1224 y procesadas adicionalmente por el procesador 1220 para obtener diversos tipos de información (por ejemplo, datos, señalización, informes, etc.). La red de acceso 120 se comunica con E-CSCF 254 y otras entidades a través de la unidad de comunicación 1226.

[172] Dentro de E-CSCF 254, el procesador 1230 realiza el procesamiento para la E-CSCF, la unidad de memoria 1232 almacena códigos de programa y datos para la E-CSCF, y la unidad de comunicación 1234 permite que la E-CSCF se comunique con otras entidades. El procesador 1230 puede realizar el procesamiento para E-CSCF 254 para los flujos de mensajes descritos anteriormente.

[173] Dentro del servidor de ubicación 286, el procesador 1240 realiza el procesamiento de ubicación y/o posicionamiento para el servidor de ubicación, la unidad de memoria 1242 almacena códigos de programa y datos para el servidor de ubicación, y la unidad de comunicación 1244 permite que el servidor de ubicación se comunique con otras entidades. El procesador 1240 puede realizar el procesamiento para el servidor de ubicación para los flujos de mensajes descritos anteriormente.

[174] Las técnicas descritas en el presente documento pueden implementarse mediante diversos medios. Por ejemplo, estas técnicas pueden implementarse en hardware, firmware, software o una combinación de ambos. Para una implementación de hardware, las unidades de procesamiento utilizadas para realizar las técnicas pueden implementarse dentro de uno o más circuitos integrados específicos de aplicación (ASIC), procesadores de señal digital (DSP), dispositivos de procesamiento de señal digital (DSPD), dispositivos lógicos programables (PLD), matrices de puertas programables in situ (FPGA), procesadores, controladores, microcontroladores, microprocesadores, dispositivos electrónicos, otras unidades electrónicas diseñadas para realizar las funciones descritas en el presente documento, o una combinación de las mismas.

[175] Para una implementación de firmware y/o software, las técnicas pueden implementarse con módulos (por ejemplo, procedimientos, funciones, etc.) que realizan las funciones descritas en el presente documento. Los códigos de firmware y/o software pueden almacenarse en una memoria (por ejemplo, la memoria 1212, 1222, 1232 y/o 1242 en la FIG. 12) y ejecutarse por un procesador (por ejemplo, procesador 1210, 1220, 1230 y/o 1240). La memoria puede implementarse dentro del procesador o fuera del procesador.

[176] Los títulos se incluyen en el presente documento para referencia y para facilitar la ubicación de ciertas secciones. Estos títulos no pretenden limitar el alcance de los conceptos descritos en el presente documento y estos conceptos pueden tener aplicabilidad en otras secciones a lo largo de toda la memoria descriptiva.

[177] La anterior descripción de los modos de realización divulgados se proporciona para permitir que cualquier experto en la materia realice o use la presente divulgación. Diversas modificaciones de estos modos de realización resultarán fácilmente evidentes a los expertos en la materia, y los principios genéricos definidos en el presente documento pueden aplicarse a otros modos de realización sin apartarse del alcance de la divulgación.

Por lo tanto, la divulgación no pretende limitarse a los modos de realización mostrados en este documento, sino que se le debe otorgar el alcance más amplio coherente con los principios y características novedosas divulgadas en el presente documento, de acuerdo con las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento realizado por el equipo de usuario (110), comprendiendo el procedimiento:

comunicarse con un subsistema multimedia de protocolo de internet (252, 254, 256, 258) de una red visitada (130) para enviar una solicitud para establecer una llamada de emergencia de voz por protocolo de Internet, en el que la solicitud comprende información de ubicación para el equipo de usuario (110);

en caso de que la información de ubicación no sea suficiente para determinar de modo único un punto de respuesta de seguridad pública, recibir instrucciones del subsistema multimedia de protocolo de internet (252, 254, 256, 258) de la red visitada para obtener y enviar, a un servidor de ubicación (272), una primera estimación de posición para el equipo de usuario (110), en el que la primera estimación de posición es suficientemente precisa para permitir que el servidor de ubicación (272) determine de modo único un punto de respuesta de seguridad pública (180); y

establecer la llamada de emergencia de voz por protocolo de internet entre el equipo de usuario (110) y el punto de respuesta de seguridad pública (180), a través de la red visitada (130).

2. El procedimiento según la reivindicación 1, que comprende además:

usar el protocolo de inicio de sesión para la llamada de emergencia de voz por protocolo de Internet;

enviar un SIP REGISTRAR para registrarse en una red doméstica (160) o en la red visitada para la llamada de emergencia por voz a través del protocolo de internet; y

enviar un SIP INVITAR como la solicitud para establecer la llamada de emergencia de voz por protocolo de internet.

3. El procedimiento según la reivindicación 1, que comprende, además: recibir desde el punto de respuesta de seguridad pública una solicitud de una estimación de posición actualizada para el equipo de usuario; y realizar el posicionamiento con el servidor de ubicación para obtener la estimación de posición actualizada.

4. Un equipo de usuario (110) configurado para:

comunicarse con un subsistema multimedia de protocolo de internet (252, 254, 256, 258) de una red visitada (130) para enviar una solicitud para establecer una llamada de emergencia de Protocolo de Voz por Internet, en el que la solicitud comprende información de ubicación para el equipo de usuario (110),

en caso de que la información de ubicación no sea suficiente para determinar de modo único un punto de respuesta de seguridad pública, recibir instrucciones del subsistema multimedia de protocolo de internet (252, 254, 256, 258) de la red visitada para obtener y enviar, a un servidor de ubicación (272), una primera estimación de posición para el equipo de usuario (110), en el que la primera estimación de posición es suficientemente precisa para permitir que el servidor de ubicación (272) determine de modo único una respuesta de seguridad pública (180),

y establecer la llamada de VoIP de emergencia entre el equipo de usuario (110) y el punto de respuesta de seguridad pública (180), a través de la red visitada (130).

5. El equipo de usuario según la reivindicación 4, configurado, además, para utilizar el protocolo de inicio de sesión para la llamada de emergencia de voz por protocolo de Internet.

6. El equipo de usuario según la reivindicación 5, configurado, además, para enviar un SIP REGISTRAR para que se registre en una red doméstica (160) para la llamada de emergencia de voz por protocolo de Internet.

7. El equipo de usuario según la reivindicación 5, configurado, además, para enviar un SIP REGISTRAR para registrarse en la red visitada para la llamada de emergencia de voz por protocolo de Internet.

8. El equipo de usuario según la reivindicación 7, en el que el SIP REGISTRAR comprende un identificador de usuario privado de emergencia formado con un nombre de dominio para la red visitada y una pseudoidentidad de abonado móvil internacional.

9. El equipo de usuario según la reivindicación 7, configurado, además, para recibir una respuesta para el SIP REGISTRAR con un identificador de usuario público temporal.

10. El equipo de usuario según la reivindicación 5, configurado, además, para enviar un SIP INVITAR como la solicitud para establecer la llamada de emergencia de voz por protocolo de Internet.

11. El equipo de usuario según la reivindicación 10, configurado, además, para enviar dicha información de ubicación para el equipo de usuario en el SIP INVITAR, y en el que la primera estimación de posición para el equipo de usuario se obtiene basándose en la información de ubicación.

12. El equipo de usuario según la reivindicación 4, configurado, además, para enviar capacidades de ubicación del equipo de usuario en la solicitud para establecer la llamada de emergencia de voz por protocolo de internet, y en el que el servidor de ubicación se selecciona basándose en las capacidades de ubicación del equipo de usuario.

13. El equipo de usuario según la reivindicación 1, en el que el servidor de ubicación se selecciona basándose en la información de ubicación.

14. El equipo de usuario según la reivindicación 1, configurado, además, para recibir del punto de respuesta de seguridad pública una solicitud de una estimación de posición actualizada para el equipo de usuario, y realizar el posicionamiento con el servidor de ubicación para obtener la estimación de posición actualizada.

15. El equipo de usuario según la reivindicación 14, configurado, además, para llevar a cabo el posicionamiento con el servidor de ubicación de acuerdo con la ubicación del plano de usuario seguro.

16. El equipo de usuario según la reivindicación 14, configurado, además, para realizar el posicionamiento con el servidor de ubicación de acuerdo con la ubicación X.S0024.

17. El equipo de usuario según la reivindicación 14, configurado, además, para realizar el posicionamiento con una red de acceso por radio (120) de acuerdo con la ubicación del plano de control 3GPP.

18. El equipo de usuario según la reivindicación 4, configurado, además, para acceder a una red de acceso por radio (120), para establecer conectividad de protocolo de internet con la red visitada a través de la red de acceso por radio, y para descubrir una dirección de protocolo de internet de un servidor local (252) para la llamada de emergencia por voz a través del protocolo de internet.

19. El equipo de usuario según la reivindicación 4, configurado, además, para acceder a una red de área local inalámbrica (120) usando un identificador de acceso de red que indica la red visitada, para establecer conectividad de protocolo de internet con la red visitada a través de la red de área local inalámbrica y para descubrir la dirección de protocolo de internet de un servidor local (252) para la llamada de emergencia de voz a través del protocolo de internet.

20. El equipo de usuario según la reivindicación 4, configurado, además, para realizar la autenticación con el servidor de ubicación.

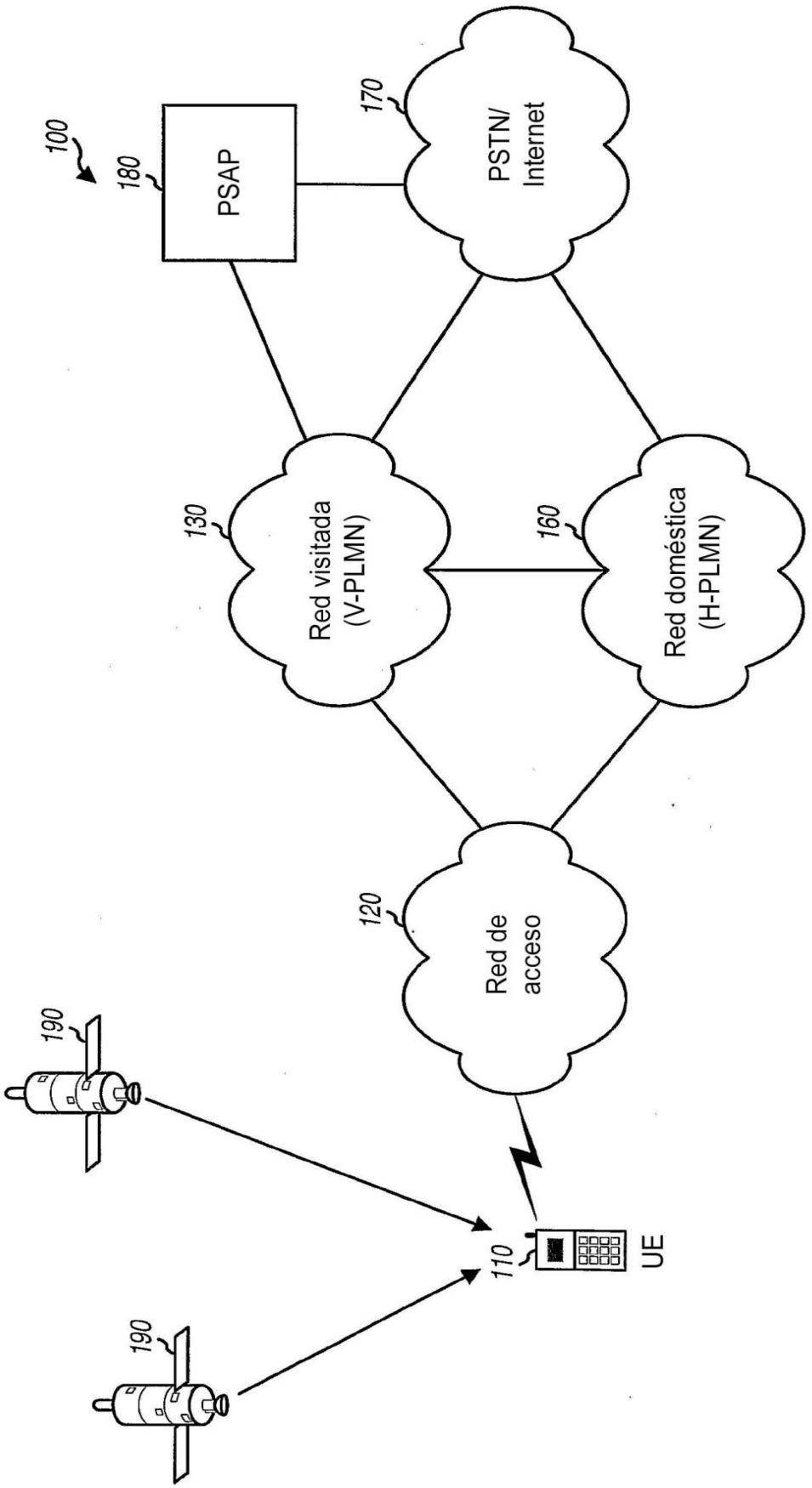
100
180
PSAP
170
PSTN/
Internet
130
Red visitada
(V-PLMN)
160
Red doméstica
(H-PLMN)
120
Red de
acceso
190
190
110
UE

FIG. 1

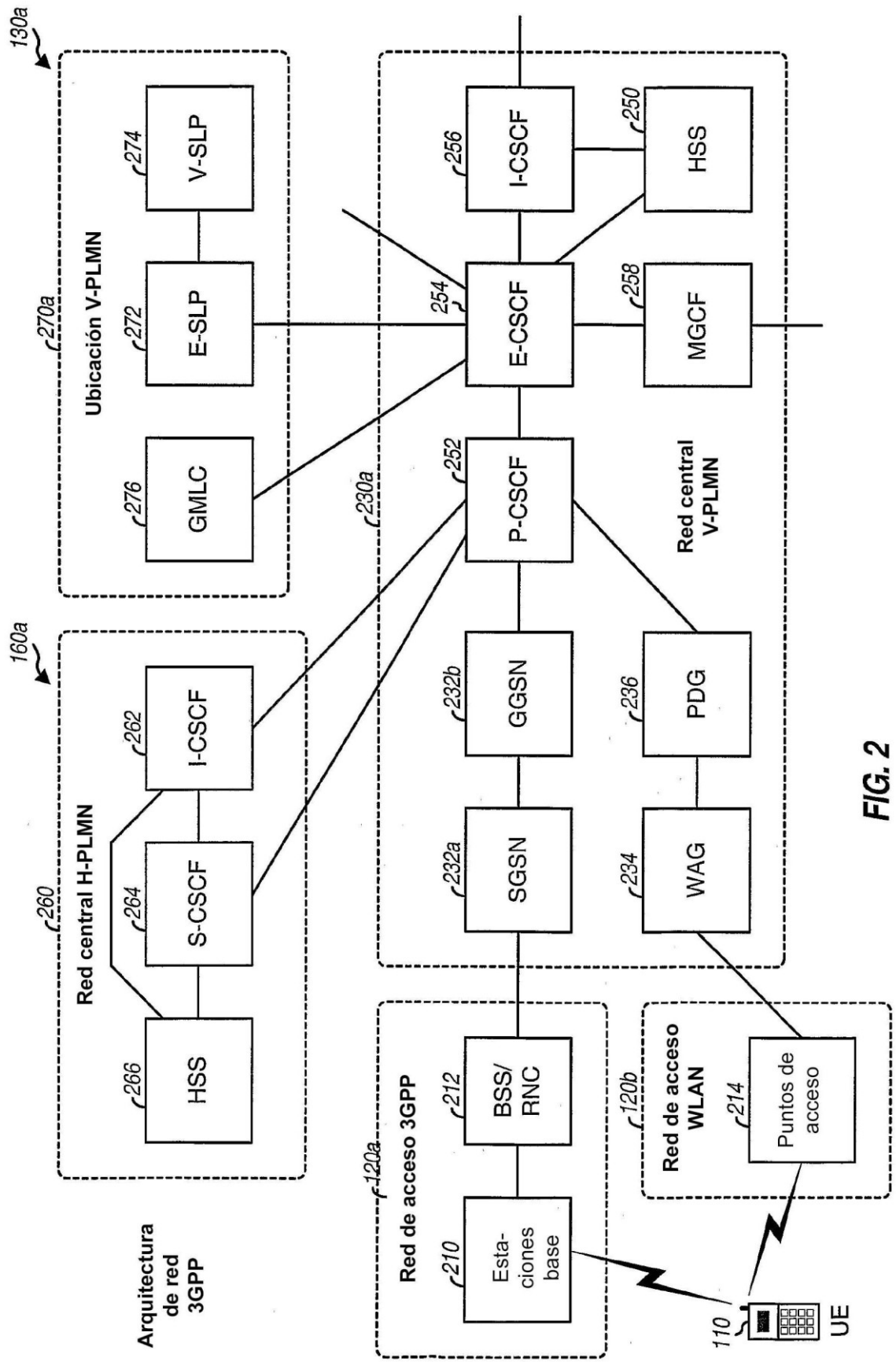
Arquitectura de red 3GPP
130a
Ubicación V-PLMN
270a
274
V-SLP
272
E-SLP
276
GMLC
160a
Red central H-PLMN
260
262
I-CSCF
264
S-CSCF
266
HSS
230a
Red central V-PLMN
254
E-CSCF
256
I-CSCF
250
HSS
258
MGCF
252
P-CSCF
232b
GGSN
232a
SGSN
236
PDG
234
WAG
120a
Red de acceso 3GPP
212
BSS/ RNC
210
Esta-ciones base
120b
Red de acceso WLAN
214
Puntos de acceso
110
UE

FIG. 2

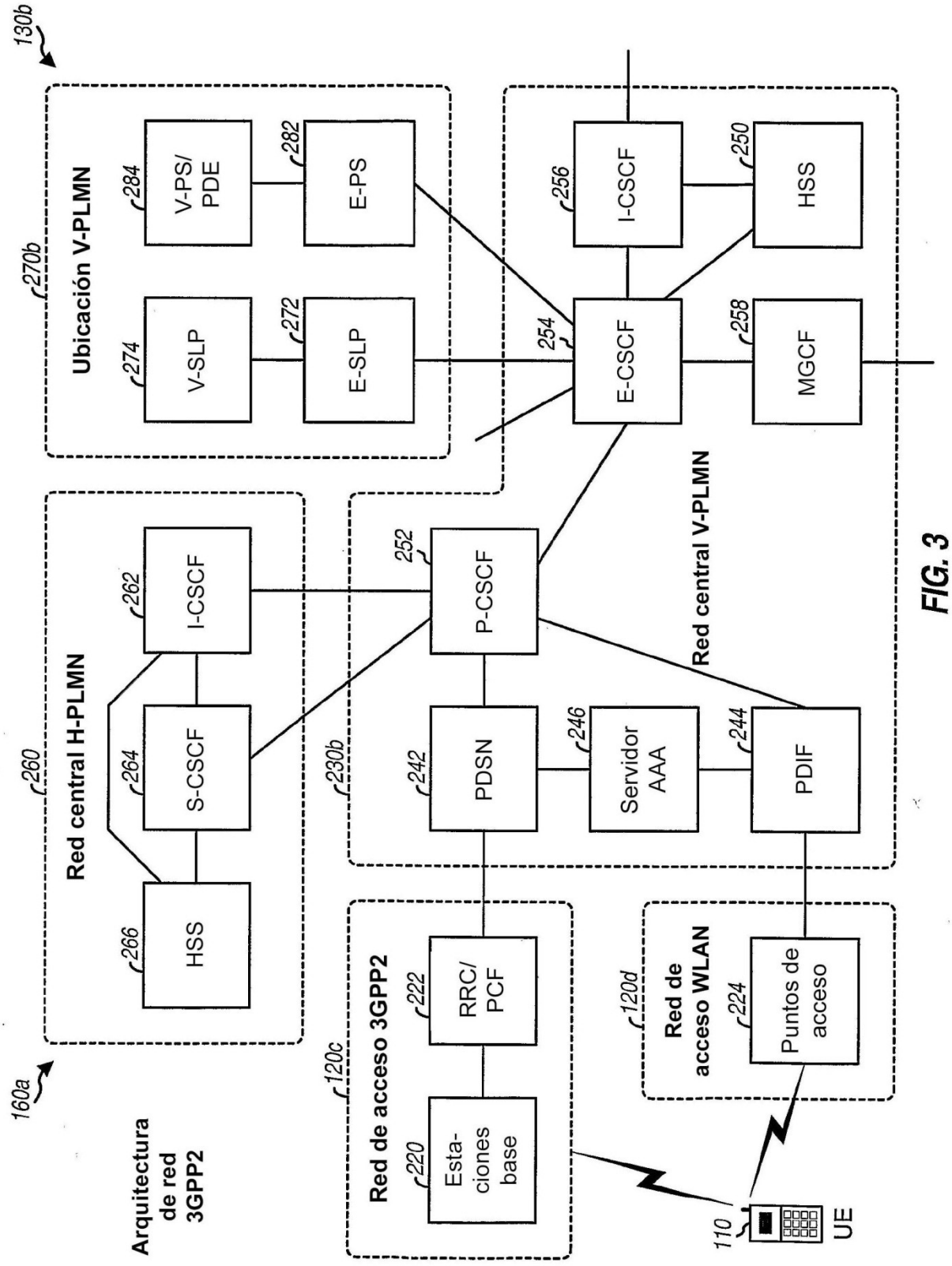
160a
Arquitectura de red 3GPP2
130b
Ubicación V-PLMN
270b
V-PS/ PDE
284
E-PS
282
V-SLP
274
E-SLP
272
Red central H-PLMN
260
I-CSCF
262
S-CSCF
264
HSS
266
Red central V-PLMN
I-CSCF
256
HSS
250
E-CSCF
254
MGCF
258
P-CSCF
252
230b
PDSN
242
Servidor AAA
246
PDIF
244
Red de acceso 3GPP2
120c
RRC/ PCF
222
Esta-ciones base
220
Red de acceso WLAN
120d
Puntos de acceso
224
110
UE

FIG. 3

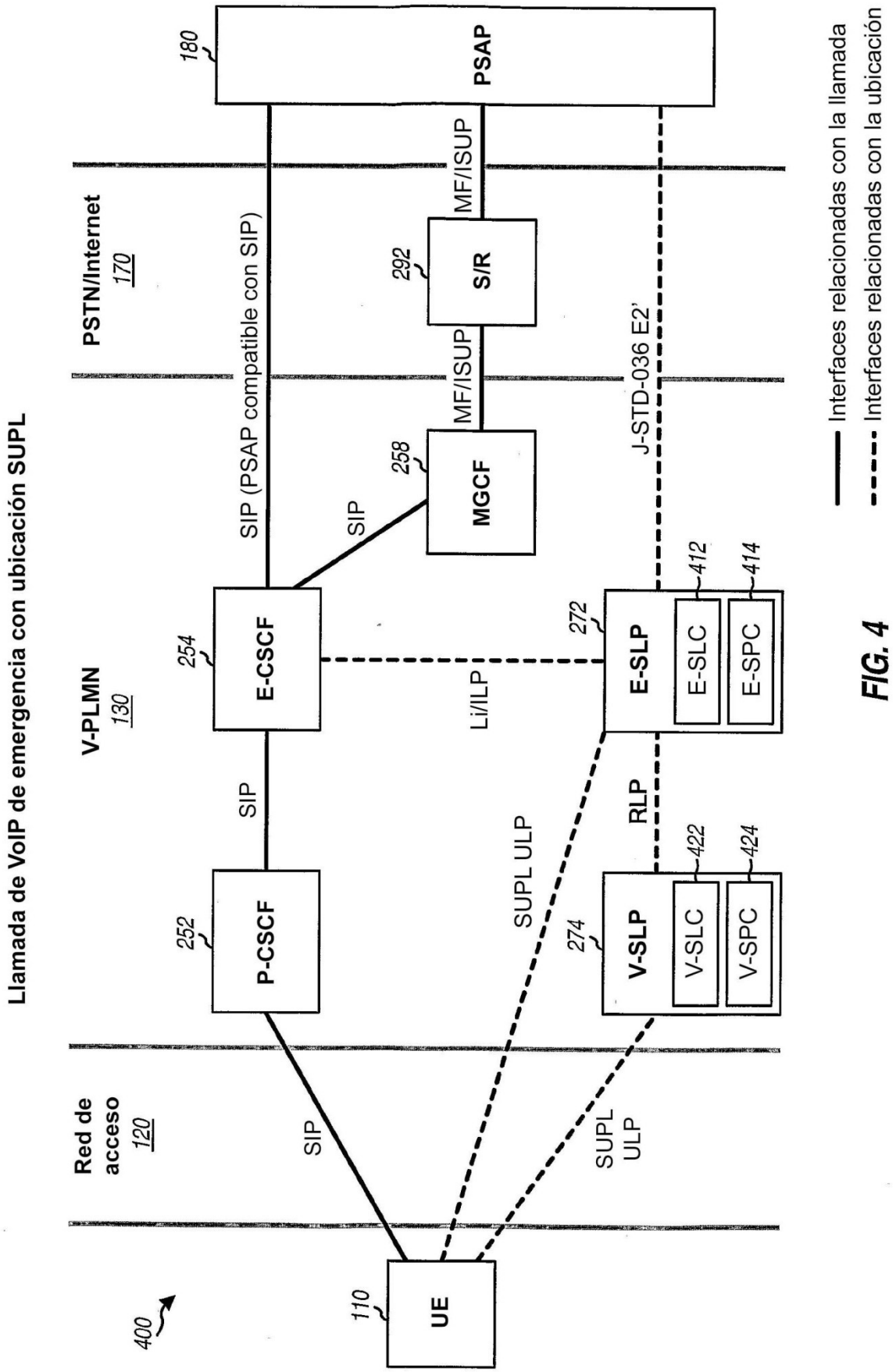
Llamada de VoIP de emergencia con ubicación SUPL
400
Red de acceso 120
V-PLMN 130
PSTN/Internet 170
UE 110
P-CSCF 252
E-CSCF 254
MGCF 258
S/R 292
PSAP 180
E-SLP 272
E-SLC 412
E-SPC 414
V-SLP 274
V-SLC 422
V-SPC 424
SIP
SIP (PSAP compatible con SIP)
MF/ISUP
MF/ISUP
SIP
Li/ILP
J-STD-036 E2'
SUPL ULP
RLP
SUPL ULP
Interfaces relacionadas con la llamada
Interfaces relacionadas con la ubicación

FIG. 4

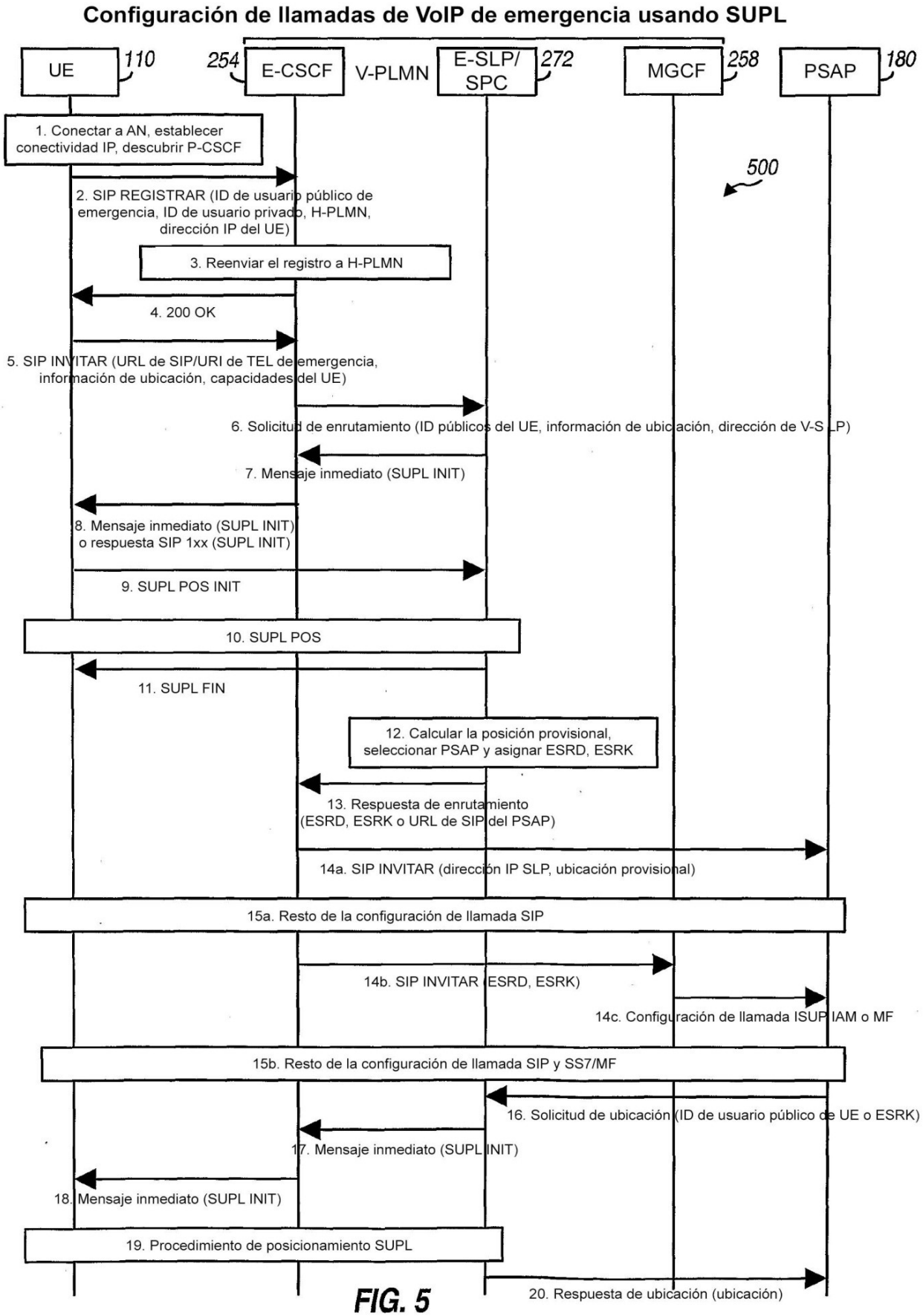
Configuración de llamadas de VoIP de emergencia usando SUPL
UE
110
254
E-CSCF
V-PLMN
E-SLP/ SPC
272
MGCF
258
PSAP
180
500
1. Conectar a AN, establecer conectividad IP, descubrir P-CSCF
2. SIP REGISTRAR (ID de usuario público de emergencia, ID de usuario privado, H-PLMN, dirección IP del UE)
3. Reenviar el registro a H-PLMN
4. 200 OK
5. SIP INVITAR (URL de SIP/URI de TEL de emergencia, información de ubicación, capacidades del UE)
6. Solicitud de enrutamiento (ID públicos del UE, información de ubicación, dirección de V-SLP)
7. Mensaje inmediato (SUPL INIT)
8. Mensaje inmediato (SUPL INIT) o respuesta SIP 1xx (SUPL INIT)
9. SUPL POS INIT
10. SUPL POS
11. SUPL FIN
12. Calcular la posición provisional, seleccionar PSAP y asignar ESRD, ESRK
13. Respuesta de enrutamiento (ESRD, ESRK o URL de SIP del PSAP)
14a. SIP INVITAR (dirección IP SLP, ubicación provisional)
15a. Resto de la configuración de llamada SIP
14b. SIP INVITAR (ESRD, ESRK)
14c. Configuración de llamada ISUP IAM o MF
15b. Resto de la configuración de llamada SIP y SS7/MF
16. Solicitud de ubicación (ID de usuario público de UE o ESRK)
17. Mensaje inmediato (SUPL INIT)
18. Mensaje inmediato (SUPL INIT)
19. Procedimiento de posicionamiento SUPL
20. Respuesta de ubicación (ubicación)

FIG. 5

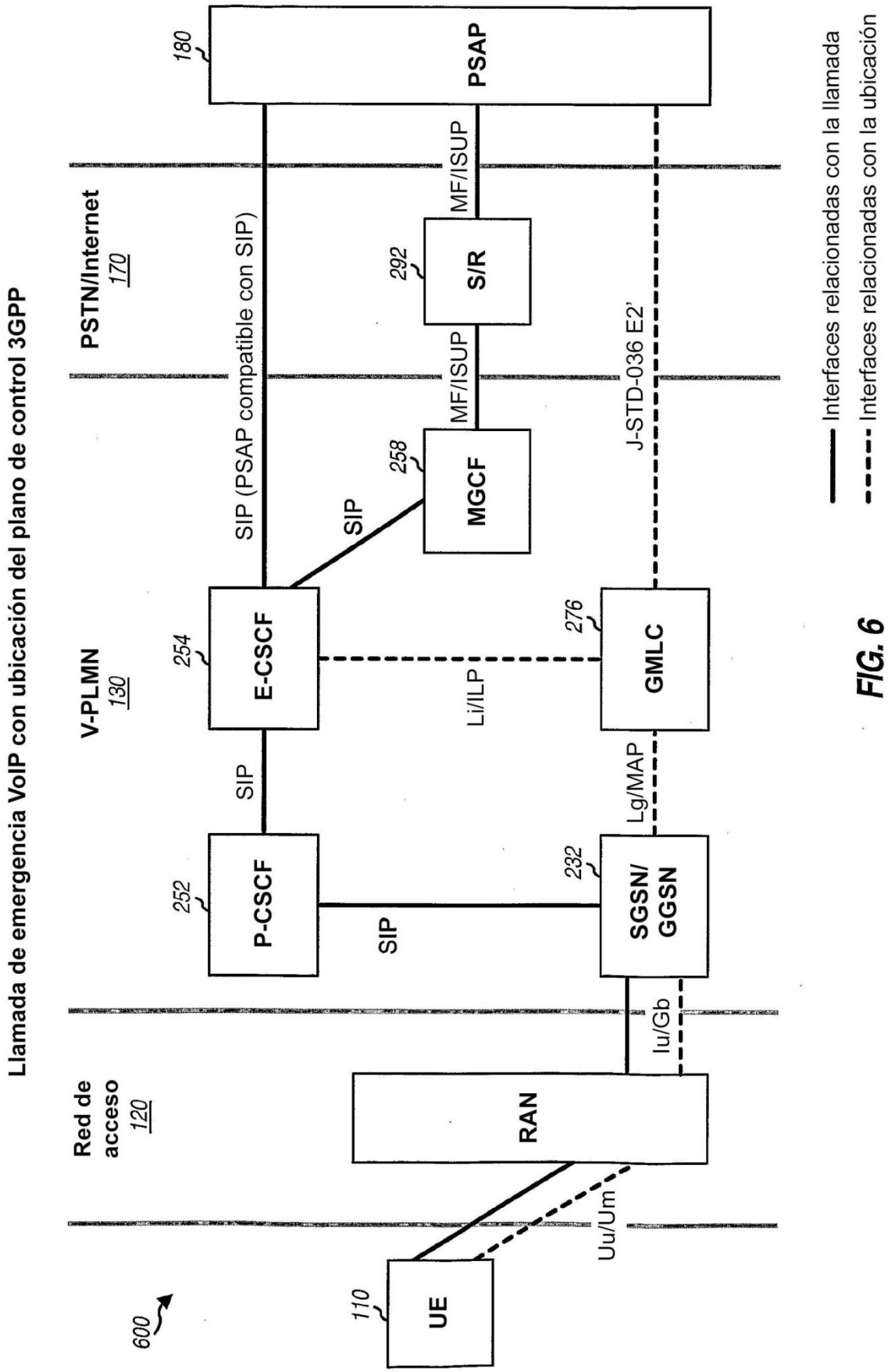
Llamada de emergencia VoIP con ubicación del plano de control 3GPP
600
UE
110
RAN
Red de acceso
120
Uu/Um
Iu/Gb
P-CSCF
252
SIP
SGSN/ GGSN
232
Lg/MAP
E-CSCF
254
SIP
Li/ILP
GMLC
276
V-PLMN
130
MGCF
258
SIP
SIP (PSAP compatible con SIP)
S/R
292
MF/ISUP
MF/ISUP
J-STD-036 E2'
PSTN/Internet
170
PSAP
180
Interfaces relacionadas con la llamada
Interfaces relacionadas con la ubicación

FIG. 6

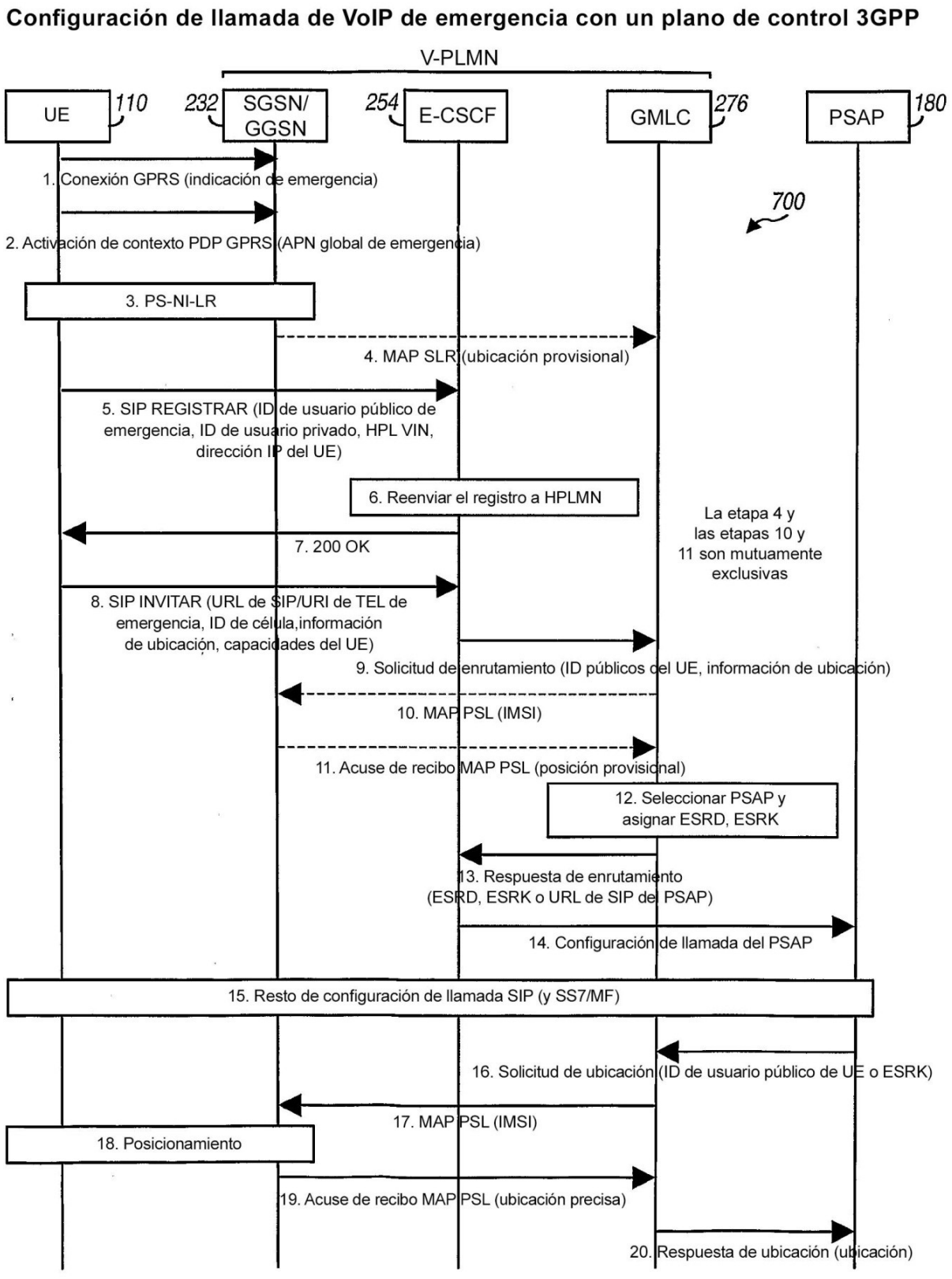
Configuración de llamada de VoIP de emergencia con un plano de control 3GPP
V-PLMN
UE
110
232
SGSN/ GGSN
254
E-CSCF
GMLC
276
PSAP
180
700
1. Conexión GPRS (indicación de emergencia)
2. Activación de contexto PDP GPRS (APN global de emergencia)
3. PS-NI-LR
4. MAP SLR (ubicación provisional)
5. SIP REGISTRAR (ID de usuario público de emergencia, ID de usuario privado, HPL VIN, dirección IP del UE)
6. Reenviar el registro a HPLMN
7. 200 OK
La etapa 4 y las etapas 10 y 11 son mutuamente exclusivas
8. SIP INVITAR (URL de SIP/URI de TEL de emergencia, ID de célula,información de ubicación, capacidades del UE)
9. Solicitud de enrutamiento (ID públicos del UE, información de ubicación)
10. MAP PSL (IMSI)
11. Acuse de recibo MAP PSL (posición provisional)
12. Seleccionar PSAP y asignar ESRD, ESRK
13. Respuesta de enrutamiento (ESRD, ESRK o URL de SIP del PSAP)
14. Configuración de llamada del PSAP
15. Resto de configuración de llamada SIP (y SS7/MF)
16. Solicitud de ubicación (ID de usuario público de UE o ESRK)
17. MAP PSL (IMSI)
18. Posicionamiento
19. Acuse de recibo MAP PSL (ubicación precisa)
20. Respuesta de ubicación (ubicación)

FIG. 7

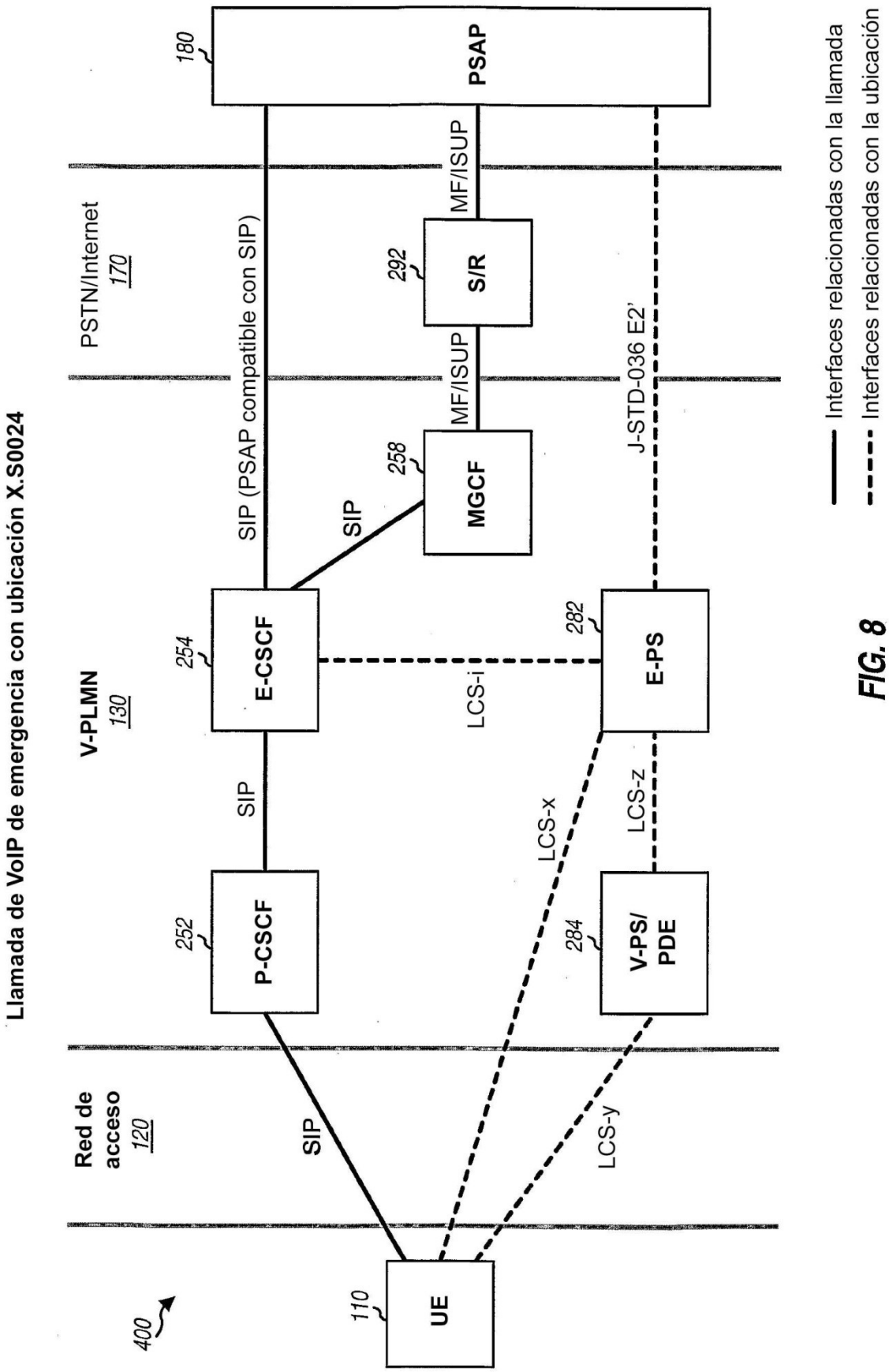
Llamada de VoIP de emergencia con ubicación X.S0024
400
UE
110
Red de acceso
120
V-PLMN
130
PSTN/Internet
170
P-CSCF
252
E-CSCF
254
MGCF
258
S/R
292
PSAP
180
V-PS/ PDE
284
E-PS
282
SIP
SIP (PSAP compatible con SIP)
MF/ISUP
MF/ISUP
LCS-i
LCS-x
LCS-y
LCS-z
J-STD-036 E2'
Interfaces relacionadas con la llamada
Interfaces relacionadas con la ubicación

FIG. 8

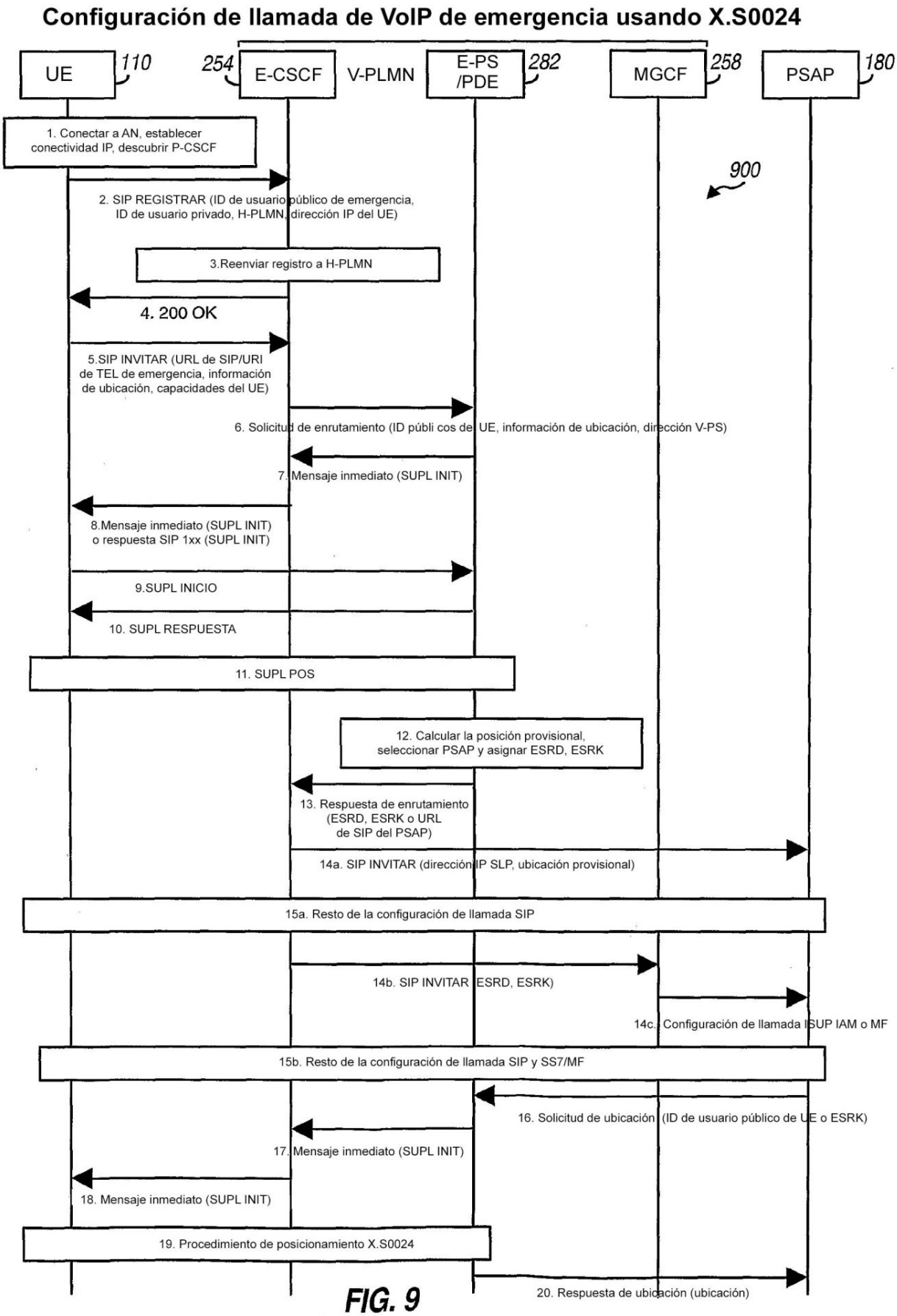
Configuración de llamada de VoIP de emergencia usando X.S0024
UE
110
254
E-CSCF
V-PLMN
E-PS /PDE
282
MGCF
258
PSAP
180
900
1. Conectar a AN, establecer conectividad IP, descubrir P-CSCF
2. SIP REGISTRAR (ID de usuario público de emergencia, ID de usuario privado, H-PLMN, dirección IP del UE)
3.Reenviar registro a H-PLMN
4. 200 OK
5.SIP INVITAR (URL de SIP/URI de TEL de emergencia, información de ubicación, capacidades del UE)
6. Solicitud de enrutamiento (ID públi cos de UE, información de ubicación, dirección V-PS)
7. Mensaje inmediato (SUPL INIT)
8.Mensaje inmediato (SUPL INIT) o respuesta SIP 1xx (SUPL INIT)
9.SUPL INICIO
10. SUPL RESPUESTA
11. SUPL POS
12. Calcular la posición provisional, seleccionar PSAP y asignar ESRD, ESRK
13. Respuesta de enrutamiento (ESRD, ESRK o URL de SIP del PSAP)
14a. SIP INVITAR (dirección IP SLP, ubicación provisional)
15a. Resto de la configuración de llamada SIP
14b. SIP INVITAR (ESRD, ESRK)
14c. Configuración de llamada ISUP IAM o MF
15b. Resto de la configuración de llamada SIP y SS7/MF
16. Solicitud de ubicación (ID de usuario público de UE o ESRK)
17. Mensaje inmediato (SUPL INIT)
18. Mensaje inmediato (SUPL INIT)
19. Procedimiento de posicionamiento X.S0024
20. Respuesta de ubicación (ubicación)

FIG. 9

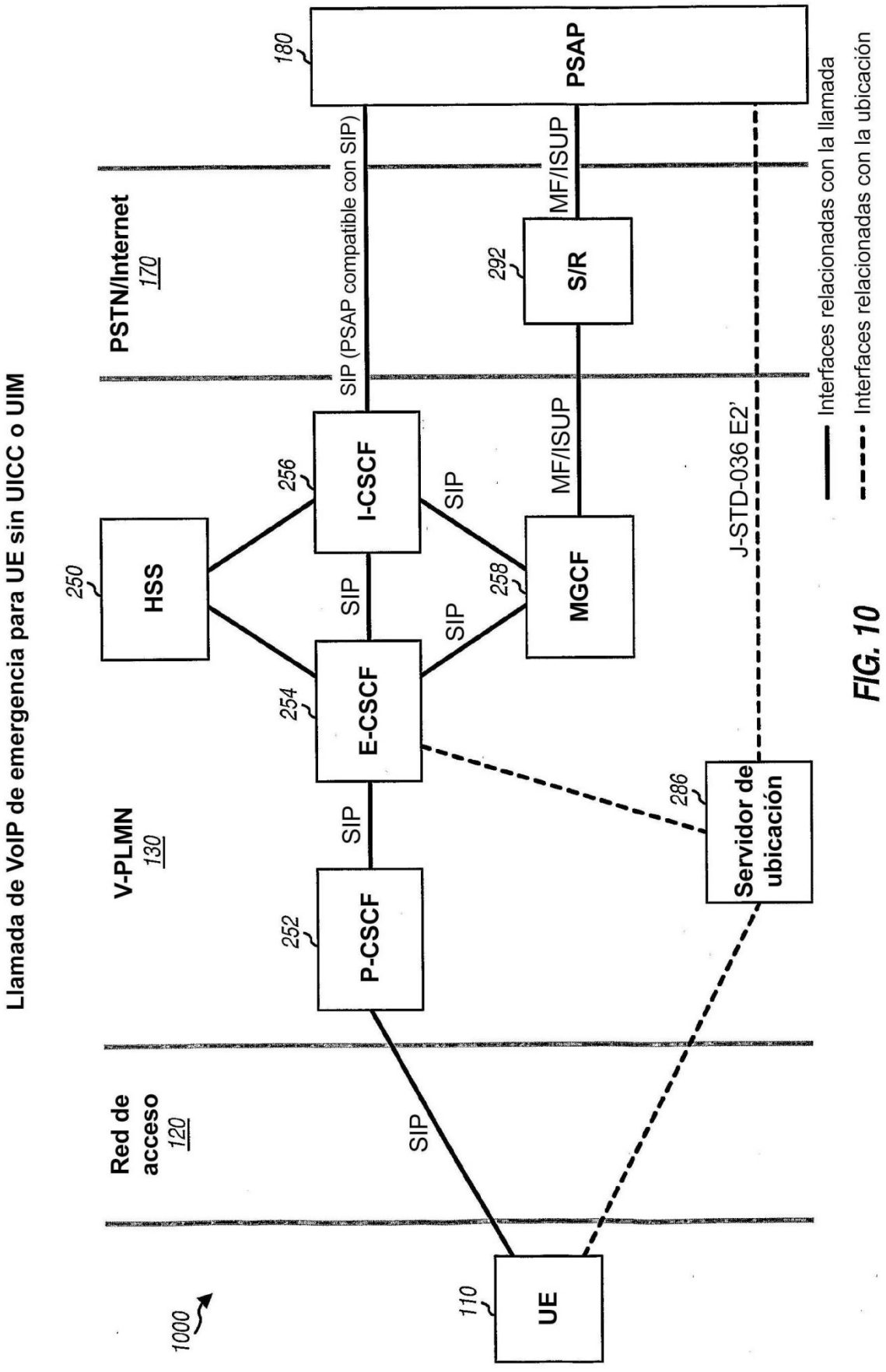
Llamada de VoIP de emergencia para UE sin UICC o UIM
1000
UE
110
Red de acceso
120
V-PLMN
130
P-CSCF
252
E-CSCF
254
I-CSCF
256
HSS
250
MGCF
258
S/R
292
PSTN/Internet
170
PSAP
180
Servidor de ubicación
286
SIP
SIP (PSAP compatible con SIP)
MF/ISUP
J-STD-036 E2'
Interfaces relacionadas con la llamada
Interfaces relacionadas con la ubicación

FIG. 10

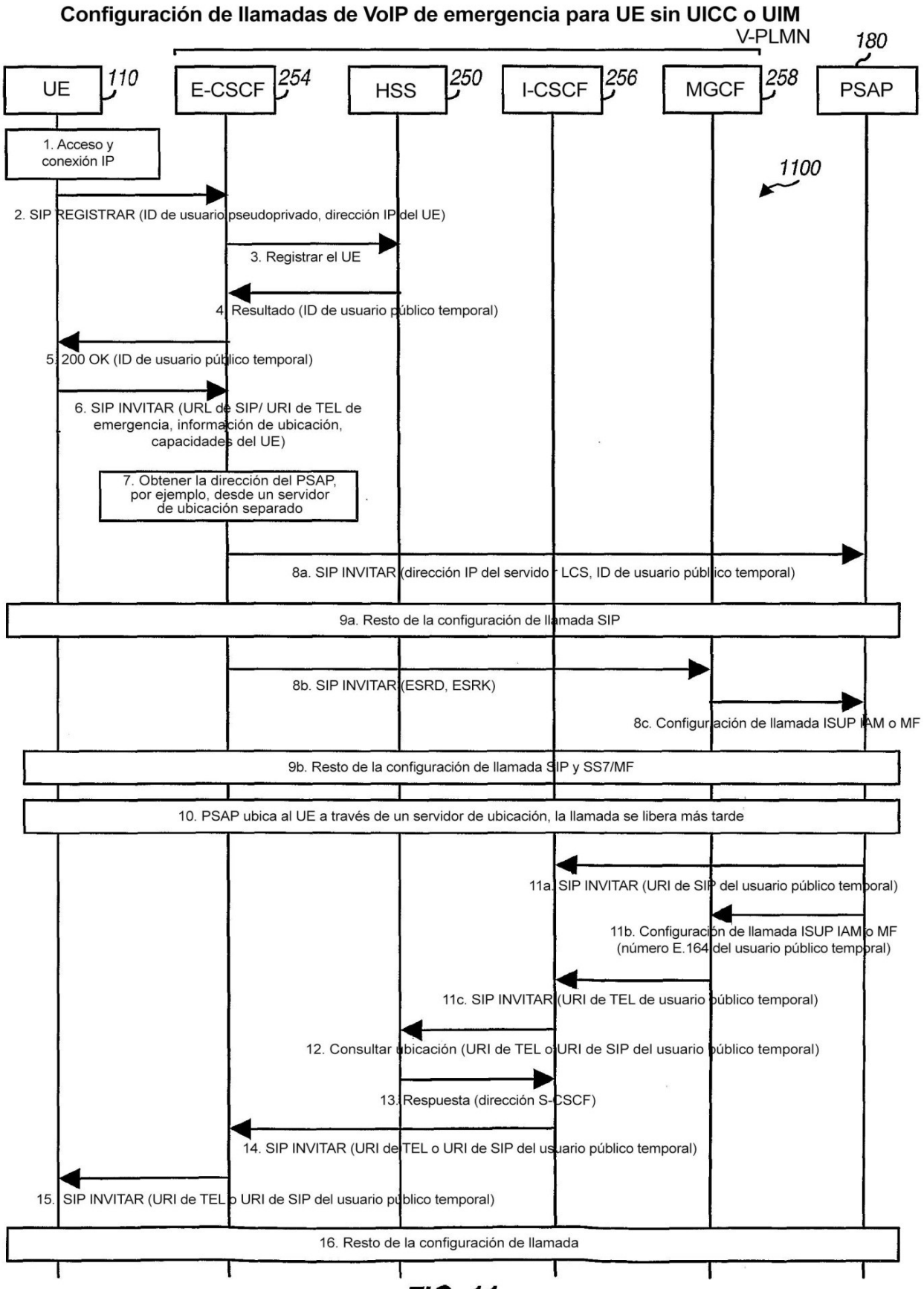
Configuración de llamadas de VoIP de emergencia para UE sin UICC o UIM
V-PLMN
180
UE
110
E-CSCF
254
HSS
250
I-CSCF
256
MGCF
258
PSAP
1100
1. Acceso y conexión IP
2. SIP REGISTRAR (ID de usuario pseudoprivado, dirección IP del UE)
3. Registrar el UE
4. Resultado (ID de usuario público temporal)
5. 200 OK (ID de usuario público temporal)
6. SIP INVITAR (URL de SIP/ URI de TEL de emergencia, información de ubicación, capacidades del UE)
7. Obtener la dirección del PSAP, por ejemplo, desde un servidor de ubicación separado
8a. SIP INVITAR (dirección IP del servidor LCS, ID de usuario público temporal)
9a. Resto de la configuración de llamada SIP
8b. SIP INVITAR (ESRD, ESRK)
8c. Configuración de llamada ISUP IAM o MF
9b. Resto de la configuración de llamada SIP y SS7/MF
10. PSAP ubica al UE a través de un servidor de ubicación, la llamada se libera más tarde
11a. SIP INVITAR (URI de SIP del usuario público temporal)
11b. Configuración de llamada ISUP IAM o MF (número E.164 del usuario público temporal)
11c. SIP INVITAR (URI de TEL de usuario público temporal)
12. Consultar ubicación (URI de TEL o URI de SIP del usuario público temporal)
13. Respuesta (dirección S-CSCF)
14. SIP INVITAR (URI de TEL o URI de SIP del usuario público temporal)
15. SIP INVITAR (URI de TEL o URI de SIP del usuario público temporal)
16. Resto de la configuración de llamada

FIG. 11

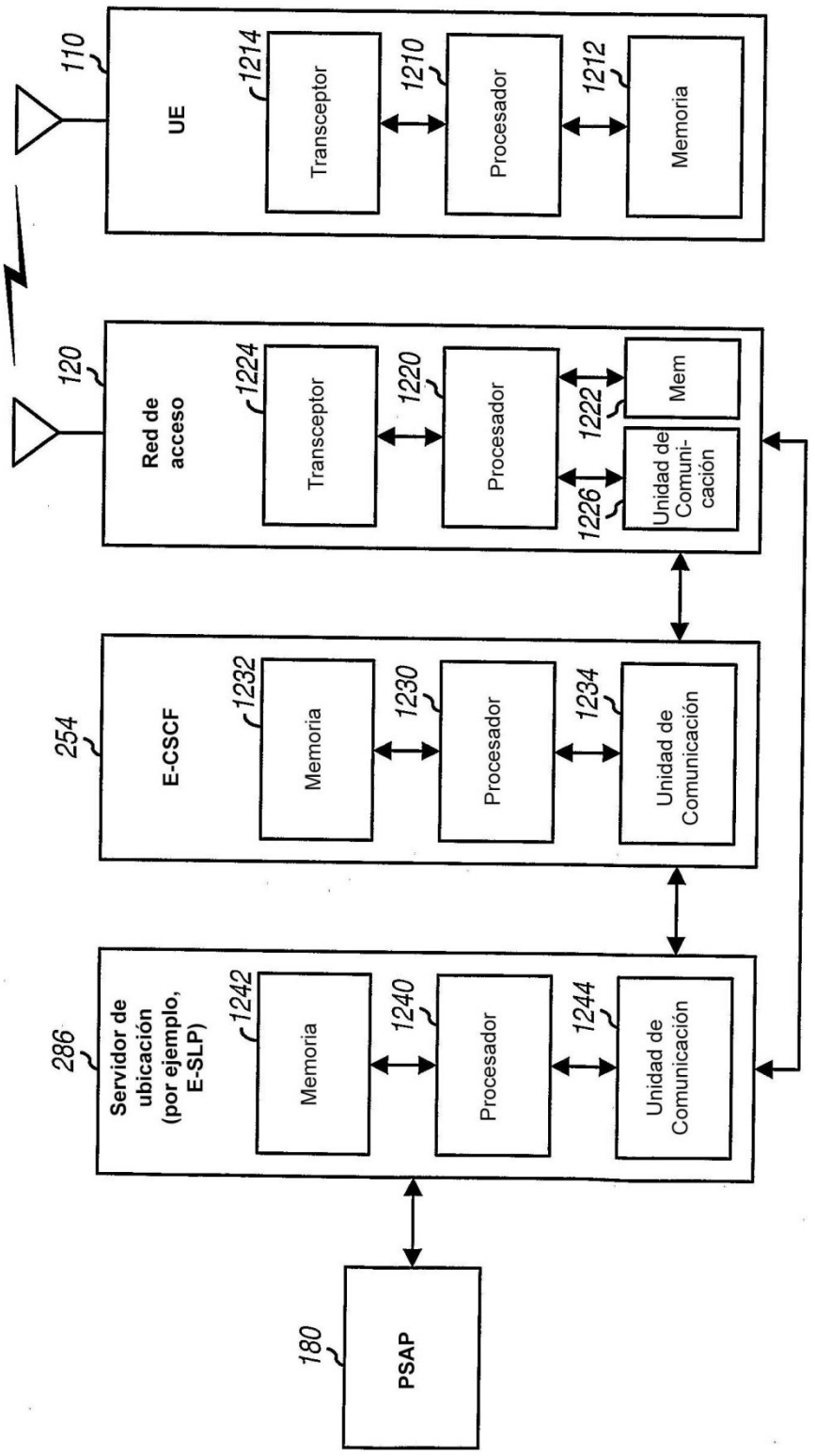
110
UE
1214
Transceptor
1210
Procesador
1212
Memoria
120
Red de acceso
1224
Transceptor
1220
Procesador
1222
Mem
1226
Unidad de Comuni-cación
254
E-CSCF
1232
Memoria
1230
Procesador
1234
Unidad de Comunicación
286
Servidor de ubicación (por ejemplo, E-SLP)
1242
Memoria
1240
Procesador
1244
Unidad de Comunicación
180
PSAP

FIG. 12