(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 381 392**

(51) Int. CI.:
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06360015 .9**
(96) Fecha de presentación: **29.04.2006**
(97) Número de publicación de la solicitud: **1850532**
(97) Fecha de publicación de la solicitud: **31.10.2007**

(54) Título: **Procedimiento de provisión a un terminal visitador de un acceso de emergencia sobre una WLAN**

(45) Fecha de publicación de la mención BOPI:
25.05.2012

(45) Fecha de la publicación del folleto de la patente:
25.05.2012

(73) Titular/es:
Alcatel Lucent
3, avenue Octave Gréard
75007 Paris , FR

(72) Inventor/es:
Selignan, Anne-Laure

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Procedimiento de provisión a un terminal visitador de un acceso de emergencia sobre una WLAN

La presente invención se refiere a un procedimiento de provisión a un terminal de un acceso de emergencia sobre una LAN inalámbrica (= WLAN), y a un sistema de comunicación para ejecutar dicho procedimiento (LAN = Red de Area Local [Local Area Network].

Las WLANs se están convirtiendo en unas redes de acceso que cada vez encuentran más favorable acogida, tanto en áreas públicas, como por ejemplo hoteles, aeropuertos, estaciones ferroviarias, instalaciones para conferencias, así como en áreas comerciales, como por ejemplo edificios de empresas. Las empresas instalan las WLANs en sus locales para permitir la libertad de movimientos de su personal proporcionando al tiempo un ancho de banda relativamente alto en comparación con las redes inalámbricas heredadas, como por ejemplo el GSM (= Sistema Global de Comunicaciones Móviles) [Global System for Mobile Communication].

Otro avance producido en los últimos años ha sido el uso creciente de las redes de datos basados en IP para la transmisión de datos en tiempo real, como por ejemplo voz y vídeo (IP = Protocolo Internet) [Internet Protocol]. Se han introducido diversos estándares que manejan aplicaciones VoIP, como por ejemplo los estándar códec G.711 y G.719, y el protocolo de transmisión RTP (VoIP = Voz sobre IP; códec = codificación / descodificación; RTP = protocolo de transporte en tiempo real) [Real Time Transport Protocol]

Hasta hace poco, los abonados utilizaban únicamente, aplicaciones no en tiempo real, por ejemplo, para conectar su buscador a Internet. Sin embargo, las WLANs actuales se encuentran con el reto de manejar, así mismo, aplicaciones en tiempo real, por ejemplo, la VoWLAN (= Voz sobre WLAN). Después de todo, los abonados una solución VoWLAN esperan las mismas calidad de voz, fiabilidad y funcionalidad que con su teléfono heredado PSTN (= Red Telefónica General de Conmutación [Public Switched Telephone Network]) o su teléfono móvil del GSM.

El documento US 2006/0068799 A1, el cual se considera como la técnica anterior más próxima, describe un sistema de acceso inalámbrico de “anfitrión abierto” que incluye un punto de acceso (AP) inalámbrico que identifica el SSID a partir de una solicitud de conexión con la WLAN. Un proveedor de servicios inalámbricos (WSP) está asociado con el SSID. El AP está acoplado a un conmutador de demarcación situado dentro del sistema de acceso. El conmutador de demarcación incluye una serie de puntos de conexión, de forma que uno o más puntos de conexión están asociados con un WSP determinado. Un WSP puede conectar un equipamiento, como por ejemplo un encaminador, con su punto o puntos de conexión asociados. El AP abre una VLAN al punto o puntos de conexión designados para establecer conexiones con el equipamiento de los WSPS en base al SSID. El WSP proporciona unas asignaciones de dirección de IP y una autenticación como un proceso nativo sobre la red, de tal manera que la experiencia del usuario puede ser personalizada por cada WSP. Pantallas de inicio de sesión y procedimientos de autenticación exclusivos pueden ser empleados por cada WSP. El sistema de acceso inalámbrico no está relacionado con el establecimiento de una llamada de emergencia . En particular, este sistema no comprende el inicio de una llamada de emergencia mediante el envío de un paquete de datos desde un terminal asociado con un SSID de emergencia seleccionado hasta uno o más puntos de acceso, de forma que los paquetes de datos son dirigidos hacia el terminal hacia una dirección de destino recibida por el terminal por medio de una solicitud del DHCP.

El documento US 2004/0066756 A1 describe un procedimiento para un equipamiento de usuario (UE) residente en una red de acceso inalámbrico (WLAN) para acceder a al menos otra red. El procedimiento incluye el almacenamiento de la identificación (SSID) de al menos otra red (PLMNs) 1 - 3 visitadas y PLMNs 4 y 5 domésticas) dentro del equipamiento de usuario. La transmisión desde el equipamiento de usuario de una solicitud para la conexión con una de la al menos otra red; lo cual incluye una identificación de al menos una de al menos otra red, con la red de acceso inalámbrica; y en respuesta a la recepción por la red de acceso inalámbrica de la identificación, el equipamiento de usuario es conectado a la al menos otra red identificada a través de la red de acceso inalámbrica. Este procedimiento no está relacionado con el establecimiento de una llamada de emergencia .

El documento US 2005/0185626 A1 describe un procedimiento para asociar una WSTA a un conjunto de servicios, en el que el conjunto de servicios es configurable en el AP. Cada conjunto de servicios es un agrupamiento arbitrario de uno o más parámetros de servicios de red, y está típicamente configurado para ya sea una LAN o bien para un anfitrión de IP de anfitrión de IP de móvil operado. Cuando una estación inalámbrica desea asociarse con un punto de acceso, el mensaje contiene el SSIP, el punto de acceso, entonces, sitúa en correspondencia el SSID con un conjunto de servicios y asocia la WSTA ya sea o bien con una subred doméstica o con una VLAN en base al SSID. Mediante la configuración local del conjunto de servicios, la VLAN por defecto y el subconjunto doméstico para una WSTA pueden ser diferentes en cada AP que la WSTA encuentra. Un servidor de seguridad está configurado con una lista de SSIDs autorizados para cada estación inalámbrica para impedir un acceso no autorizado a una VLAN o a una subred doméstica.

El documento US 2004/0181692 A1 describe un sistema de comunicación de una red de área local inalámbrica (WLAN) que incluye un punto de acceso en comunicación con una estación móvil y al menos un servidor de Autenticación, Autorización y Contabilización (AAA) proporciona un procedimiento de autenticación por medio del

cual un usuario de la estación móvil puede seleccionar un proveedor de servicios de la WLAN entre uno o más proveedores de servicios de la WLAN y / o uno o más proveedores de servicios de 3GPP antes de ser autenticados y, así mismo, para adoptar una decisión para abonarse a los servicios del proveedor de servicios seleccionados en base a la información de los servicios de la red, distintos de o además de un Identificador de Red Inalámbrica (SSID), asociado con el proveedor de servicios seleccionados. El sistema no utiliza el DHCP.

Stefano M. Faccin: "Propuesta WiNOT TGu para el Requisito de los Servicios de Emergencia" ["WiNOT TGu Proposal for Emergency Services Requirement "] IEEE 802.11 – 06/0288R1, 6 de marzo de 2006 (03-06-2006). páginas 1 a 9, XP0024118839 IEEE P802.11 LANs Inalámbricas especifica una propuesta para hacer frente al requisito de los servicios de emergencia en los requisitos de agrupamiento genéricos para el estándar IEEE 802.11 u.

Hepworth et al.: "Propuesta Tgu para el soporte E911" ["Tgu Proposal for E911 support"], IEEE 802.11 – 06/280R0, 17 de febrero de 2006 (17-02-2006) páginas 1 a 12, XP002418840 IEEE P Nos. 802.11 LANs Inalámbricas propone, como en una red celular, que un usuario puede hacer uso del servicio de llamadas de emergencia ya sea utilizando las credenciales existentes, ya sea utilizando un mecanismo de acceso autenticado. Uno de los problemas relacionados con la seguridad es que el usuario autenticado no debe ser capaz de interferir con el tráfico difundido de los demás usuarios, pero necesita contar con un soporte de difusión (para el DHCP, el ARP, etc.). La solución a ello es que el servicio de emergencia necesita ser suministrado sobre un AP virtual separado. Esto significa que el tráfico de difusión de los usuarios de emergencia está separado de los usuarios normales (y el usuario autenticado no necesita su clave de grupo). En concreto, la solución debe asegurar que los usuarios de emergencia no autenticados no puedan interferir con el tráfico difundido (como por ejemplo el DHCP, el ARP) de los demás usuarios autenticados. No se describe el uso de un "SSID de emergencia".

Stephenson, Dave: "Solicitud de Ancho de Banda Acelerada" ["Expedited Bandwidth Request"] IEEE 802.11 – 06/0268RO, 17 de febrero de 2006 (17-02-2066) páginas 1 a 21, XP002418841 IEEE 802.11 describe lo que puede considerarse como una propuesta completa para el requisito R911. Esta propuesta se divide en dos partes. Parte 1: la señalización desde una QSTA a un QAP para identificar la información adicional acerca de la naturaleza de la solicitud de ancho de banda (incluyendo si es una llamada de emergencia). Parte 2: la propuesta para suministrar un servicio 911 a clientes que presenten únicamente credenciales de seguridad públicas.

Hepworth, Montemurro, Rudolf: "Propuesta para el Soporte de Servicios de Emergencia" ["Proposal for Emergency Service Support"] IEEE 802.11 – 06/0450RO, 6 de marzo de 2006 (06-03-2006), páginas 1 a 13, XP002418842 IEEE 802.11 da respuesta al requisito R911 define la funcionalidad del IEEE802.11 que se requeriría para soportar y un servicio de Llamadas de Emergencia como parte de una solución multinivel global.

El documento US 2005/0181805 A1 describe un procedimiento y un sistema para la localización de un abonado de acceso móvil sin licencia (UMA). El procedimiento permite que sea localizado un usuario de una estación móvil que comprende un aparato telefónico o dispositivo similar que soporta un acceso de voz y datos por medio tanto de unos espectros de voz con licencia como sin licencia. De acuerdo con ello, se puede acceder a servicios que requieren una información de localización, como por ejemplo servicios 911 al operar la estación móvil con arreglo a sesiones tanto UMA como de redes inalámbricas con licencia (por ejemplo celulares).

El documento US 2005/0190892 A1 describe que, con el fin de que los vehículos de servicios de emergencia puedan ser despachados al destino correcto de forma inmediata, se necesita una información precisa acerca del emplazamiento del llamante. Otro problema se refiere a las llamadas de emergencia de encaminamiento al destino correcto. Para las llamadas de emergencia se utiliza un código universal, como por ejemplo el 911 en Norteamérica y el 112 en Europa. Este código universal no puede ser utilizado para identificar el destino de la llamada. Estos problemas son particularmente acuciantes en sistemas de comunicaciones erráticos, como por ejemplo respecto de redes de comunicaciones de protocolos de voz sobre Internet. Esto se debe a que los terminales de los usuarios cambian el emplazamiento de la red. Estos problemas se resuelven haciendo posible que el emplazamiento geográfico del llamante de emergencia sea determinado por entidades situadas dentro de una red a base de paquetes sin necesidad de modificar la infraestructura existente de la red de servicios de emergencia.

El documento US 6 714 536 B1 describe unos procedimientos y unos aparatos para hacer posible el establecimiento de una conexión de paquetes de datos mediante el envío de una indicación de una dirección de red a través de una vía telefónica. En una primera forma de realización, una pila de protocolos inicia el establecimiento de una conexión con Internet mediante el envío de un segmento de datos a través de una vía telefónica de una red telefónica general de conmutación (PSTN) y, a continuación, opera y mantiene la conexión con Internet en una conexión de paquetes separada. Los dígitos de marcación son utilizados para indicar la dirección de una computadora remota o de un dispositivo inalámbrico a través de la vía telefónica. La presente invención permite, así mismo, llamadas telefónicas multimedia mezcladas PSTN / Internet. En una forma de realización ejemplar, cuando se establece una conexión telefónica de PSTN punto a punto, automáticamente aparece una pantalla de información en uno o ambos extremos de la conexión vía Internet.

Constituye el objetivo de la presente invención garantizar a un terminal visitador el acceso a los servicios de comunicación para fines de emergencia.

El objetivo de la presente invención se obtiene mediante un procedimiento de provisión a un terminal de un acceso de emergencia sobre una WLAN a una LAN que comprenda uno o más puntos de acceso y una función de control de acceso la cual admite paquetes de datos procedentes de usuarios de la WLAN asociados con un primer SSID a la LAN, en el que el procedimiento comprende las etapas de: la definición de uno o más SSIDs de emergencia dedicados a posibilitar el acceso a la LAN en un caso de emergencia; el inicio de una llamada de emergencia mediante el envío de un paquete de datos a un terminal asociado con un SSID de emergencia seleccionado a uno de los uno o más puntos de acceso de forma que los paquetes de datos son dirigidos por el terminal hacia una dirección de destino recibida por el terminal por medio de una respuesta del DHCP; la admisión, por medio de la función de control de acceso, de los paquetes de datos desde el terminal asociado con el SSID de emergencia seleccionado hacia la LAN; y el encaminamiento de los paquetes de datos asociados con el SSID de emergencia seleccionado, después de la admisión en la LAN, hacia un punto de respuesta de emergencia, en el que el procedimiento comprende las etapas adicionales de: la solicitud por el terminal de una opción de DHCP particular que provea al terminal de una dirección de IP de un gestor de llamadas responsable de la gestión del establecimiento de una llamada de emergencia hacia el punto de respuesta de emergencia y un punto de conexión sobre el cual el gestor de llamadas está escuchando; la recepción, por el terminal, de la dirección de IP del gestor de llamadas y del punto de conexión sobre el cual el gestor de llamadas está escuchando por medio del DHCP desde un servidor del DHCP; y el direccionamiento de los paquetes de datos al terminal asociado con el SSID de emergencia seleccionado con la dirección de IP recibida del gestor de llamadas y el punto de conexión sobre el cual está escuchando el gestor de llamadas (SSID = Identificador de Red Inalámbrica [Service Set Identifier]).

La asociación de un terminal con un SSID significa que el terminal notifica dentro de la comunicación sobre la interfaz aérea de la WLAN dicho SSID. De modo preferente, el SSID es notificado dentro de la parte del nivel de MAC de la comunicación sobre la interfaz aérea. Eso significa que el terminal señaliza, durante la comunicación sobre la interfaz aérea un SSID al punto de acceso, el SSID que está asociado con el terminal.

De acuerdo con la presente invención, los paquetes de datos desde el terminal asociado con el SSID de emergencia seleccionado son encaminados, después de la admisión en la LAN, hacia un punto de respuesta de emergencia.

La presente invención ofrece un procedimiento sencillo de la forma de proveer a un terminal – tanto a un terminal visitador como a un terminal autorizado – de un acceso fiable y seguro sobre una WLAN a una LAN en el caso de una emergencia.

Un usuario de un terminal móvil no está limitado a las LANs públicamente accesibles para establecer una llamada de emergencia sino que puede, así mismo, utilizar LANs corporativas o comerciales, por ejemplo una red corporativa universitaria. De esta manera, incluso un terminal visitador, el cual normalmente no estaría autorizado a acceder a una red con derechos de acceso restringidos, puede establecer una llamada de emergencia a través de la red.

Así mismo, la presente invención contribuye de manera significativa a la aceptación futura de la técnica VoWLAN, dado que la presente invención provee a una WLAN de unos medios para ofrecer conectividad y fiabilidad en el caso de una emergencia. En los EE..UU., la Comisión Federal de Comunicaciones (= FCC) requiere que los proveedores de los servicios VoIP aseguren que todas las llamadas VoIP interconectadas proporcionan una total capacidad respecto del número 9 – 1 – 1, siendo el 9 – 1 – 1 el número de emergencia oficial nacional en los EE.UU. y Canadá. Similares requisitos se contemplan en muchos países europeos en los que el número de emergencia nacional oficial es el 1 – 1 – 2, por ejemplo. Por medio de la presente invención, cualquier llamante que marca el número de emergencia central 9 – 1 – 1 y / o 1 – 1 - 2 puede estar seguro de ser transferido de manera fiable hacia un PSAP (= Punto Contestador de Seguridad Pública [Public Safety Answering Point]) desde el cual se organizará la ayuda.

Para el encaminamiento de paquetes de datos relacionados con la llamada de emergencia, existen disponibles diversos procedimientos. Por consiguiente, un procedimiento adecuado puede ser elegido dependiendo de la situación efectiva y de las circunstancias, como por ejemplo la infraestructura, la carga de tráfico, etc., disponibles.

Otras ventajas se obtienen mediante las formas de realización de la invención indicadas por las reivindicaciones dependientes.

De acuerdo con la invención, el terminal que desea iniciar una llamada de emergencia, recibe, por medio de una indagación del DHCP, una dirección de destino a la que enviar los paquetes de datos correspondientes (DHCP = Protocolo de Configuración Dinámica de Servidores [Dynamic Host Configuration Protocol]). Por consiguiente, el terminal dirige los paquetes de datos desde el terminal asociado con el SSID de emergencia seleccionado con la dirección de destino recibida a través de la solicitud del DHCP.

El concepto DHCP puede ser realizado por medio de un servidor del DHCP el cual es, de modo preferente, implementado como un duende y espera en el punto de conexión 67 del UDP las solicitudes de clientes (UDP = Protocolo de Datagramas de Usuario [User Datagram Protocol]). Un archivo de configuración del servidor del DHCP comprende la información acerca de la batería de direcciones que van a ser distribuidas así como los datos adicionales acerca de los parámetros relevantes de la red. Por consiguiente, un terminal con emplazamientos a menudo cambiantes puede prescindir de una preconfiguración de propensión al error. El terminal simplemente establece una conexión con la WLAN y solicita todos los parámetros relevantes del servidor del DHCP.

A continuación, los paquetes de datos procedentes del terminal asociado con el SSID de emergencia seleccionado son enviados por el terminal a la dirección de IP y al punto de conexión de un gestor de llamadas el cual encaminará los paquetes de datos relacionados con la llamada de emergencia hacia un PSAP. El terminal recibe la dirección relacionada con los datos del gestor de llamadas procedentes del servidor del DHCP.

El terminal solicita una opción particular del DHCP que provea al terminal de la dirección de destino, esto es, una dirección de IP del gestor de llamadas. El terminal puede enviar un mensaje asociado con el procedimiento del DHCP a un servidor del DHCP para solicitar una dirección de destino a la que enviar los paquetes de datos de la llamada de emergencia. Después de la recepción de la dirección de destino procedente del servidor del DHCP, el terminal asociado con el SSID de emergencia seleccionado establece la dirección de IP recibida como dirección de destino de los paquetes de datos desde el terminal asociado con el SSID de emergencia seleccionado. La dirección de destino comprende la dirección de IP del gestor de llamadas y un punto de conexión sobre el que está escuchando el gestor de llamadas.

En otra forma de realización preferente, la señalización de las llamadas de acuerdo con la presente invención está en conformidad con todo tipo de clientes de gestión de llamadas, como el SIP, el H.323, etc. (SIP = Protocolo de Inicio de Sesión [Session Initiation Protocol]). El procedimiento actual es totalmente un protocolo agnóstico. El terminal solo tiene que enviar paquetes de RTP al gestor de llamadas. No hay ningún códec ni ninguna negociación de entramado.

De acuerdo con una forma de realización preferente de la invención, los paquetes de datos desde un terminal asociado con un SSID de emergencia son encaminados, una vez que han sido admitidos en una red LAN, hacia un servicio de emergencia o hacia un punto de respuesta de emergencia, por ejemplo un PSAP. De modo preferente, el encaminamiento es ejecutado por una PBX o por el gestor de llamadas. Una vez que el gestor de llamadas recibe una llamada de emergencia, el gestor de llamadas establece una llamada relativa al área geográfica de la llamada original. Todos los paquetes de datos asociados con el terminal asociado por SSID de emergencia que entran en la LAN son encaminados hacia el servicio de emergencia del punto de llamada de emergencia, de modo preferente, con carácter independiente con respecto de la dirección de destino originalmente indicada de los paquetes de datos. Los paquetes de datos procedentes de un terminal asociado con un SSID de emergencia tienen acceso garantizado a la LAN solo a los fines de establecer una llamada de emergencia.

En línea con la invención dicha LAN puede ser una LAN accesible por medio de dos o más WLANs. Cada una de las WLANs pueden servir como una red de acceso al entorno LAN y estar asociada con un SSID separado. Entonces, la LAN puede ser accesible a través de una primera WLAN por medio de un primer SSID, por ejemplo un SSID normal, y accesible a través de una segunda WLAN por medio de un segundo SSID, por ejemplo un SSID de emergencia.

De forma correspondiente, la invención presenta, así mismo, un procedimiento para proporcionar acceso a una LAN accesible por medio de al menos dos WLANs, para una pluralidad de terminales de usuario que comprenda terminales de usuarios autorizados, por ejemplo, usuarios pertenecientes a una corporación, así como terminales de usuarios visitadores. Dicha primera WLAN proporciona acceso a la LAN para paquetes de datos asociados con un primer SSID. Los paquetes de la primera WLAN son filtrados utilizando un procedimiento de encriptación para permitir solo paquetes de datos adecuadamente encriptados desde terminales de usuarios autorizados hacia la LAN y descartar paquetes de datos procedentes de otros terminales. Así mismo, al menos una segunda WLAN proporciona acceso a la LAN para paquetes de datos procedentes de terminales de todos los usuarios y asociados con un segundo SSID. Los paquetes de datos procedentes de la segunda WLAN son filtrados para permitir solo paquetes de datos que incorporen llamadas de emergencia de VoID.

Dado que los clientes asociados con un SSID de emergencia pueden ser usuarios visitadores, no puede establecerse la encriptación o la autenticación. Para impedir ataques a o un uso no autorizado del SSID de emergencia, pueden establecerse diversos medios de seguridad.

Una información importante con la que contar en un servicio de emergencia es la localización de un usuario que inicia una llamada de emergencia. Con la ayuda de un rastreador del DHCP y con el uso de los servicios web albergados en un servidor de localización, esta información puede ser transmitida al PSAP.

En una forma de realización preferente, se definen los SSIDs de emergencia específicos para llamadas de emergencia, junto con capacidades específicas, como por ejemplo códec. Cada uno de los SSIDs de emergencia definidos está asociado con diferentes capacidades, por ejemplo un códec diferente. Por tanto, pueden ser configurados diversos SSIDs de emergencia dependiendo de los parámetros que serán utilizados para la llamada, por ejemplo, un SSID de emergencia para el G.711 y otro SSID de emergencia para el G.729. El usuario del terminal o la inteligencia del terminal puede seleccionar un SSID de emergencia dependiendo de las capacidades asociadas. La información acerca de las capacidades asociadas con un SSID de emergencia específico puede ser extraída de la difusión de un SSID de emergencia. La información acerca de las capacidades puede estar contenida en el propio SSID o puede ser recuperada de un elemento de información separado de la LAN. El gestor de llamadas recibe la información acerca del procesamiento de los paquetes de datos en la cabecera del RTP.

De modo preferente, una llamada de emergencia se inicia mediante el envío de paquetes de datos asociados con una llamada telefónica de VoWLAN. La VoWLAN permite VoIP en un entorno móvil. Se basa en unas WLANs basadas en el estándar 802.11 del IEEE, en la mayoría de los casos dentro de edificios. La VoWLAN comprende la integración de sistemas tales como el VoIP en base a los protocolos de señalización de llamadas, como por ejemplo el SIP o el H.323, y la WLAN de acuerdo con el estándar 802.11 del IEEE en la versión de 802.11e el cual soporta la Calidad de Servicio (= QoS). Así mismo, una conexión directa con las redes del UMTS es posible y, por tanto, la expansión de los servicios VoWLAN fuera del alcance de las LANs basadas en radio.

De acuerdo con otra forma de realización preferente de la invención, el terminal usa un procedimiento estándar 802.11e o WMM para indicar que el flujo de datos relacionado con la llamada de emergencia tiene una prioridad de emergencia de voz (WMM = WiFi Multi Media; WiFi = Fidelidad Inalámbrica [Wirless Fidelity]). El control de admisión de las llamadas a una red es negociado por el uso de la TSPEC (= Especificación de Tráfico [Traffic Specification}). Una estación, en este caso el terminal, especifica sus requisitos de flujo de tráfico (tasa de transmisión de datos, límites de retardo, tamaño de los paquetes, y otros) y solicita un QAP (= Punto de Acceso a QoS [QoS Access Point]) para crear una TPSC mediante el envío de la trama de acción de gestión de la ADDTS (= TSPEC adicionales [ADD TSPEC]). El QAP calcula la carga existente en base al conjunto actual de TSPECs emitidos. En base a las condiciones actuales, el QAP puede aceptar o denegar la nueva solicitud de TSPEC. Si la TSPEC es denegada, no se permite la categoría de acceso de alta prioridad dentro de la Estación de QoS (= QSTA) para utilizar los parámetros de acceso de esta prioridad, pero en su lugar debe utilizar los parámetros de nivel de QoS.

Así mismo, puede ser utilizado el desalojo para favorecer una llamada de emergencia. Cuando un usuario del terminal marca un número prioritario, como por ejemplo un número de emergencia, la parte que llama puede esperar que la WLAN procese la llamada urgente con una prioridad más elevada que una conversación normal de un abonado. El AP y / o el gestor de llamadas reconoce el estado de prioridad de la llamada de emergencia y desaloja los recursos asignados de llamadas de prioridad menor que la llamada de emergencia a favor de la llamada de emergencia. En general, los mecanismos de desalojo y de TSPEC pueden ser utilizados para garantizar una QoS específica a los paquetes de datos asociados con una llamada de emergencia.

De modo preferente, el terminal comprende una unidad de representación como por ejemplo, una pantalla, donde un símbolo específico, por ejemplo las letras “SOS” o un icono que represente una luz de una patrulla de policía, puede mostrarse sobre una pantalla blanda (Sfotscreen) o sobre un tablero de móvil, cuando el terminal detecta que está disponible un SSID de emergencia. Como alternativa, una señal acústica, como por ejemplo un tintineo o un sonido específico, es reproducido desde un altavoz del terminal en el caso de que se encuentre disponible un SSID de emergencia. Un archivo de datos que comprenda iconos o el sonido específicos puede estar almacenado en una memoria del terminal y puede ser recuperado de la memoria y generado de salida en el terminal para informar a un usuario del terminal de que se encuentra disponible un acceso de emergencia a la WLAN.

De acuerdo con otra forma de realización de la invención, al menos uno de los uno o más puntos de acceso difunden los uno o más SSIDs. El terminal detecta al menos uno de los uno o más SSIDs de emergencia difundidos y selecciona un SSID de emergencia entre el al menos un SSID de emergencia detectado.

El objetivo de la presente invención se consigue, así mismo, mediante un sistema de comunicación para proveer a un terminal de un acceso de emergencia sobre una WLAN a una LAN, comprendiendo el sistema de comunicación una función de control de acceso la cual admite paquetes de datos procedentes de usuarios de la WLAN asociados con el primer SSID en la LAN, en el que el sistema de comunicación comprende una interfaz adaptada para recibir paquetes de datos procedentes de un terminal apropiado con un SSID de emergencia seleccionado entre el al menos un SSID de emergencia detectado, una unidad de control adaptada para reenviar los paquetes de datos recibidos desde el terminal asociado con el SSID de emergencia seleccionado hacia la función de control de acceso, de forma que la función de control de acceso permite los paquetes de datos procedentes del terminal asociado con el SSID de emergencia seleccionado hacia la LAN, y en el que el sistema de comunicación está adaptado para encaminar los paquetes de datos desde el terminal asociado con el SSID de emergencia seleccionado, después de la admisión en la LAN, hacia un punto contestador de emergencia de forma que dichos paquetes transportan una dirección de destino recibida en el terminal procedente del sistema de comunicación por medio de una respuesta del DHCP, y de forma que el sistema de comunicación comprende así mismo un gestor de llamadas responsable de la gestión del establecimiento de una llamada de emergencia hacia el punto contestador de emergencia y un servidor del DHCP adaptado para proveer, en respuesta a una solicitud del terminal respecto de una opción correspondiente concreta del DHCP, al terminal de una dirección IP del gestor de llamadas y un punto de conexión sobre el cual está escuchando el gestor de llamados por medio del DHCP para direccionar los paquetes de datos al terminal asociado con el SSID de emergencia seleccionado con la dirección IP recibida del gestor de llamadas y el punto de conexión sobre el cual está escuchando el gestor de llamadas.

El sistema de comunicación está adaptado para encaminar los paquetes de datos procedentes de un terminal asociado con el SSID de emergencia seleccionado cuando los paquetes de datos han sido dirigidos al terminal con una dirección de destino recibida en el terminal por medio de una solicitud del DHCP.

De modo preferente, el sistema de comunicación comprende así mismo un emisor adaptado para difundir uno o más SSIDs de emergencia dedicados para posibilitar el acceso a la LAN en un caso de emergencia hacia el terminal.

Las referidas, así como otras características distintivas y ventajas de la invención se apreciarán en mayor medida mediante la lectura de la descripción detallada subsecuente tomada en combinación con los dibujos que se acompañan, en los cuales:

La Figura 1 es un diagrama de bloques de un terminal que accede a una LAN de acuerdo con una forma de realización de la invención.

La Figura 2 es una secuencia de flujo de mensajes que muestra un terminal que accede a una LAN de acuerdo con una forma de realización de la invención.

Las Figuras 3a a c son secuencias de flujo de mensajes que muestran opciones de encaminamiento.

La Figura 4 es un diagrama de bloques de terminales que acceden a una LAN de acuerdo con otra forma de realización de la invención.

La Figura 5 es otro diagrama de bloques de terminales que acceden a una LAN de acuerdo con otra forma de realización más de la invención.

Las Figuras 6a a d son secuencias de flujo de mensajes que muestran opciones relacionadas con la localización.

La Figura 1 muestra un sistema de comunicación 1 que comprende una WLAN 2, una LAN 3, una red 5, un gestor de llamadas 40, y un PSAP 60. Un usuario 100 de un terminal 10 quiere conectarse por medio de una llamada de emergencia con un PSAP 60. El terminal 10 está situado dentro del área de cobertura de un punto de acceso 20 el cual pertenece a la LAN 3. La LAN 3 comprende así mismo una función 21 de control de acceso, un servidor 30 del DHCP, un servidor de localización 31, y un gestor de llamadas 40. La Red 5 conecta con el gestor de llamadas 40 y con el PSAP 60. La segunda red 5 puede ser una red telefónica ordinaria, como por ejemplo una red PSTN.

El terminal 10 puede ser un dispositivo móvil para establecer una llamada de telecomunicación por medio de una red de acceso. Puede ser, por ejemplo, un teléfono móvil o una computadora portátil que comprenda un cliente de VoIP con una interfaz de WLAN. El terminal 10 comprende una unidad de detección 101, una unidad de control 102 y una interfaz de usuario 103. La interfaz de usuario 103 comprende unos medios para posibilitar que el usuario 100 provea al terminal 10 de una entrada y para recibir la salida procedente del terminal 10. De modo preferente, la interfaz de usuario 103 comprende un teclado con unas teclas de entrada, un micrófono, una pantalla y un altavoz.

El punto de acceso 20 de la LAN 3 es un dispositivo hardware o un software informático que actúa como un concentrador de comunicaciones para que el terminal 10 conecte con la WLAN 2. El AP 20 comprende un remitente 201, un modulo de interfaz 202 con una interfaz con la WLAN 2 y una interfaz con la LAN 3, y una unidad de control 203. La interfaz con la WLAN 2 es capaz de enviar y recibir, esto es intercambiar, datos con los terminales de la WLAN, la interfaz con la LAN 3 es capaz de enviar y recibir, esto es, intercambiar, datos con los elementos de red de la LAN 3.

El remitente 201 difunde uno o más SSIDs de emergencia dedicados para permitir el acceso a la LAN 3 en un caso de emergencia. La interfaz 202 recibe los paquetes de datos enviados por el terminal 10 a través de la interfaz aérea con la LAN 3. La unidad de control 203 proporciona una función de control e inteligencia con el punto de acceso 20.

La WLAN 2 puede estar representada por los terminales situados dentro del área de cobertura del remitente, la interfaz con la WLAN 2, y el medio que acarrea el intercambio de datos entre los terminales y la interfaz con la WLAN 2, esto es la interfaz aérea.

Un SSID identifica una red de radio en base al estándar 802.11 del IEEE. El SSID, conocido también como nombre de red porque esencialmente es un nombre que identifica una red, es una cadena sensible a un supuesto unívoco de hasta 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos de una WLAN deben emplear el mismo SSID con el fin de comunicarse entre sí. El SSID está configurado en un AP de una WLAN y se establece por todos los clientes que desean acceder a la WLAN a través del AP. El SSID sobre los clientes inalámbricos puede establecerse ya sea de forma manual, introduciendo el SSID en las configuraciones de red del cliente o bien de manera automática, dejando el SSID sin especificar o en blanco.

La función 21 de control de acceso, proporciona un acceso a la LAN 3. La función 21 de control de acceso puede llevarse a cabo como un controlador de la WLAN, de modo preferente como un dispositivo autónomo, o puede ser integrado en la funcionalidad dispuesta por el AP 20 y / o por el dispositivo AP. La funcion 21 de control de acceso comprende una unidad de control 204 para el control de la función 21 de control de acceso y la aplicación, a los paquetes de datos que llegan a los bordes de la WLAN 2, las normas de control de acceso almacenadas en un módulo de memoria 205. La función 21 de control de acceso filtra los paquetes de datos que llegan antes de admitirlos a las redes 2 y 3.

La WLAN 2 está conectada al servidor 30 del DHCP, al servidor 31 de localización, y al gestor de llamadas 40 por medio de la red 3, la cual es una red de IP, por ejemplo una LAN o Internet por medio de una función de retransmisión del DHCP. El servidor 30 del DHCP asigna direcciones de IP dinámicas a los dispositivos que acceden

a la LAN. Con un direccionamiento dinámico, un dispositivo puede tener una dirección de IP diferente cada vez que se conecta a una red. En algunos sistemas la dirección de IP de un dispositivo puede incluso cambiar mientras sigue estando conectada. El DHCP soporta, así mismo, una mezcla de direcciones IP estáticas y dinámicas.

El servidor 35 de localización alberga servicios, de modo preferente servicios web, para localizar la disposición del terminal 10. Esto puede conseguirse extrayendo información de los datos recibidos del terminal 10. Toda la información adaptada para proporcionar todos los datos del terminal 10 se resumen mediante el término "información de localización". La información de localización puede ser útil para localizar el terminal 10.

El gestor de llamadas 40 es responsable para gestionar un establecimiento de llamadas de emergencia mediante el PASP 60. El gestor de llamadas 40 está compuesto por una o varias computadoras entrelazadas, esto es, una plataforma hardware, una plataforma software basada en la plataforma hardware y varios programas de aplicación ejecutados por la plataforma del sistema formados por la plataforma software y hardware. Las funcionalidades del gestor de llamadas 40 se suministran mediante la ejecución de estos programas de aplicación. Los programas de aplicación o una parte seleccionada de estos programas de aplicación constituyen un producto de software informático que proporciona un servicio de gestor de llamadas tal y como se describe a continuación, cuando es ejecutado en la plataforma del sistema. Así mismo, dicho producto de software informático está constituido por un medio de almacenamiento que almacena estos programas de aplicación o dicha parte seleccionada de los programas de aplicación.

La Figura 2 muestra una secuencia de mensajes entre el terminal 10, el punto de acceso 20 de la LAN 2, el servidor 30 del DHCP, el gestor de llamadas 40 y el PSAP 60 de acuerdo con una primera forma de realización de la invencion. En una primera etapa 901, dos SSIDs de emergencia dedicados a un servicio de emergencia son difundidos por el AP 20 de una forma en la que el terminal 10 pueda detectar los SSIDs de emergencia por medio de una unidad de detección. Después de la detección de los SSIDs de emergencia difundidos por el terminal 10, un modelo de icono es representado sobre una unidad de representación del terminal en acción 902 para informar a un usuario del terminal 10 que el servicio de emergencia está disponible en la actual localización. Como alternativa, el usuario puede ser informado acerca de la disponibilidad del servicio de emergencia por medio del mecanismo de información.

Para solicitar el servicio de emergencia indicado, el usuario del terminal 10 puede, en la etapa 903, marcar, en un teclado del terminal 10, un número de servicio de emergencia asociado con un servicio de emergencia, por ejemplo el número 9-1-1 en Norteamérica o el número 1-1-2 en Europa, o presionar una tecla programable dedicada al servicio de emergencia dispuesto sobre el terminal 10. La tecla programable es una tecla situada por debajo del panel de representación final del terminal que lleva a cabo funciones especiales.

Desencadenado por la acción 903, el terminal 10 selecciona un SSID de emergencia entre el conjunto de SSIDs de emergencia detectados. Como alternativa, el usuario del terminal es inducido a elegir un SSID de emergencia de acuerdo con sus preferencias y a indicar su elección introduciéndola por medio de una tecla. De la manera correspondiente, el terminal 10 se asocia con el SSID de emergencia seleccionado en la etapa 904. El códec utilizado para la llamada de emergencia puede ser el G.711, de acuerdo con el SSID de emergencia seleccionado. Si el terminal 10 estuvo originariamente asociado con otro SSID, el terminal 10 debe desasociarse del antiguo SSID y asociarse con el SSID de emergencia. En la etapa siguiente 905, el terminal 10 envía un mensaje DHCP DISCOVER, al servidor 30 del DHCP.

El servidor 30 del DHCP contesta a la solicitud del DHCP con un mensaje 906, por ejemplo un mensaje DHCP OFFER, enviado al terminal 10 en el que el mensaje 906 comprende una dirección de IP y un punto de conexión del gestor de llamadas 40 y una dirección de IP del terminal 10. El terminal puede escoger la oferta, enviar otra solicitud al servidor del DHCP y recibir un mensaje de confirmación. De esta manera, el terminal 10 es habilitado para enviar un flujo 907 de RTP que comprenda paquetes de datos en el estándar códec G.711 al destino especificado, esto es, el gestor de llamadas 40. Dado que los paquetes de datos enviados del flujo 907 de RTP están asociados con el SSID de emergencia seleccionado, la función 21 de control de acceso los deja pasar.

Todos los paquetes de datos que entran en la LAN 3 a través del AP 20 deben pasar la función 21 de control de acceso la cual puede ser implementada como un servidor de control de acceso autónomo dedicado. El servidor de control de acceso puede estar compuesto por una o varias computadoras entrelazadas, esto es, una plataforma hardware, una plataforma software en base a la plataforma hardware y varios programas de aplicación ejecutados por la plataforma del sistema formados por la plataforma software y hardware. La función 21 de control de acceso es suministrada por la ejecución de estos programas de aplicación. Los programas de aplicación o una parte asociada con estos programas de aplicación constituyen un producto de software informático que proporciona un servicio de control de acceso de acuerdo con lo descrito más adelante, cuando son ejecutados en la plataforma del sistema. Así mismo, dicho producto de software informático está constituido por un medio de almacenamiento que almacena dichos programas de aplicación o una parte seleccionada de dichos programas de aplicación.

Así mismo, es posible que la función 21 de control de acceso sea implementada en un elemento de red de la LAN 3 como una tarea adicional, por ejemplo, en un conmutador, centralita o encaminador de la LAN 3. Así mismo, es posible que la función 21 de control de acceso esté incluida dentro del AP 20. En el caso de que la función 21 de

control de acceso sea implementada en un elemento de red convencional de la LAN 3, la función 21 de control de acceso puede estar incluida dentro de un módulo específico que proporcione la funcionalidad de control de acceso en cooperación con otros módulos y unidades del elemento de red.

La función 21 de control de acceso lee la cabecera de cada paquete de datos que llega, en particular el SSID comprendido dentro de la cabecera, y controla si el SSID está autorizado en la LAN 3. Por ejemplo, la función 21 de control de acceso está configurada para admitir todos los paquetes de datos asociados con el primer SSID utilizado por usuarios autorizados de la LAN 3 y cualquiera de los SSIDs de emergencia difundidos. Con este fin, la función 21 de control de acceso puede tener almacenado en la memoria 205 un archivo de datos que comprenda una lista de control de acceso con una lista de SSIDs que estén aprobados. A continuación, la función 21 de control de acceso consulta la lista de control de acceso y compara el SSID de un paquete de datos llegado con los SSIDs de dicha lista de control de acceso. Dependiendo del resultado, el paquete de datos es admitido en la LAN 3 o rechazado. De manera similar, el procedimiento de la ACL mencionado con anterioridad puede ser llevado a cabo por medio de la función 21 de control de acceso (ACL = Lista de Control de Acceso [Access Control List]).

Otra forma de controlar el acceso a la LAN 3 puede ser asignar, mediante la función 21 de control de acceso un ancho de banda limitado a un cliente que envía paquetes de datos asociados con un SSID de emergencia. De modo preferente, la función 21 de control de acceso concluye un contrato con cada cliente que envía paquetes de datos asociados con un SSID de emergencia. Este contrato limita el ancho de banda aceptado por un cliente. De esta manera, los paquetes de datos enviados por el terminal que excedan del ancho de banda asignado son simplemente descolgados por la función 21 de control de acceso. Esto disminuye el peligro de que un usuario utilice su acceso a la WLAN para enviar otros paquetes de datos distintos de los paquetes de datos relacionados con una llamada de emergencia.

La función 21 de control de acceso, puede, así mismo, filtrar los paquetes de datos asociados con un SSID de emergencia de acuerdo con el protocolo y con las direcciones de IP de origen y con las direcciones de IP de destino utilizadas. Por ejemplo, es posible permitir solo paquetes de datos que acarreen comunicación de voz. En general, es posible solo filtrar los paquetes de datos con respecto al servicio / protocolo y / o ancho de banda y / u origen y / o destino.

Aparte del terminal 10 y su asignación a una dirección de IP por medio de una solución del DHCP, el terminal 10 puede, así mismo, recibir una dirección de IP por otros procedimientos conocidos en el campo de la conexión en red de las telecomunicaciones.

El procedimiento por medio del cual los paquetes de datos asociados con la llamada de emergencia son transmitidos al gestor de llamadas 40 como una primera estación, es totalmente independiente del protocolo asociado. Para asegurar una transmisión fiable y rápida, todas las modificaciones que son propensas a errores, como por ejemplo la codificación y la descodificación, entramado, etc. se omiten. Los paquetes de datos son simplemente transferidos, por ejemplo, como paquetes RTP, desde el terminal 10 hasta el gestor de llamadas 40 el cual siempre escucha una solicitud del servicio de emergencias sobre un punto de conexión específico.

Desde el gestor de llamadas 40, los paquetes de datos relacionados con la llamada de emergencia son encaminados, a través de una red PSTN, hacia el PSAP 60. Por consiguiente, la marcación 903 de un número del servicio de emergencia rápidamente conecta el terminal 10 con un despachador situado en un PSAP entrenado para encaminar la llamada de emergencia hacia los organismos sanitarios, antincendios y de seguridad de emergencia locales.

En el centro 60 de llamadas, del PSAP, un operador verifica la localización de la llamada, determina la naturaleza de la emergencia y decide cuales son los equipos de la emergencia que deben ser notificados. El despachador de la emergencia utiliza la información de la localización suministrada por los LBS para dirigir al personal de seguridad pública que responde a la emergencia para asegurar un tiempo de respuesta de la emergencia lo más corto posible (LBS = Servicios Basados en la Localización {[Location Based Services]). Algunas veces un solo PSAP primario contestará para una zona entera. En la mayoría de los casos, el llamante es transferido a un PSAP secundario desde el cual se enviará ayuda. Los PSAPs secundarios están algunas veces situados en oficinas de avisos de incendios, cuarteles generales de policía municipal o en centros de envío de ambulancias. Una vez que la llamada ha sido procesada, el operador PSAP o el centro de despacho alerta al equipo de respuesta de la emergencia apropiado, ya se trate de un incendio, un rescate o de un asunto de la policía.

Dado que no es conocido que el terminal 10 sea accesible a la LAN 3 por medio del AP 20, no puede utilizar la encriptación. Sin embargo, hay varias formas de proteger a la LAN 3 de la piratería y / o de ataques.

El principal riesgo para la seguridad es la negación del servicio (= DoS). Un ataque de DoS es un ataque a un anfitrión (servidor) con el fin de paralizar uno o más de sus servicios. Normalmente, esto se consigue porsobrecarga. Típicamente los ataques DoS no se llevan a cabo a mano sino con un programa subrepticio el cual se propaga de manera independiente hacia otros anfitriones de una red. De esta manera, el atacante tiene anfitriones adicionales asumiendo la ejecución para sus ataques DoS. En una infraestructura del estándar 802.11, como por ejemplo la LAN 3, las normas de protección de seguridad pueden ser aplicadas para conseguir una cierta protección contra los

ataques. Solo los paquetes del DHCP y del RTP son flujos autorizados para un anfitrión específico de la LAN 3. Si se utilizan otros protocolos, el usuario puede ser preterido y no se puede asociar con el AP 20 durante un periodo de tiempo configurable.

Como alternativa, puede ser implementada una aplicación de detección y defensa de DoS y Hombre en el Medio (= MITM) sobre la LAN 3. Un ataque MITM tiene su origen en un atacante situado física o lógicamente en el medio de los copartícipes en las comunicaciones. En esta posición, el atacante MITM tiene un control total sobre el tráfico de datos entre los dos o más abonados de la red y puede ver o incluso manipular a voluntad la información intercambiada.

Otra forma más de proteger la LAN 3 contra los ataques sería proporcionar solo un ancho de banda limitado para los usuarios: Esto puede ayudar a que el sistema se defienda contra los ataques DoS. Así mismo, es posible que la NAT de destino utilizada para impedir el ataque sea dirigida contra otros servicios (NAT = Traducción de Direcciones de Red [Network Address Traslation]).

En otra forma de realización más, una asociación de todos los usuarios visitantes puede ser utilizada en una red de área local virtual (= VLAN) dedicada a ellos con el fin de aplicar la ACL por cada VLAN. Una VLAN sobre una red es un dominio de radiodifusión. Todos los anfitriones dispuestos sobre esa VLAN pueden comunicar con los demás miembros de la misma VLAN. Una VLAN privada (= PVLAN) permite que el tráfico sea segmentado como nivel de enlace de datos (nivel 2) del modelo OSI, limitando el tamaño del dominio de radiodifusión (OSI = Interconexión de Sistemas Abiertos [Open Systems Interconnection]). La ACL está configurada, por ejemplo, en un encaminador el cual puede excluir el acceso de clientes específicos a la LAN 3 por medio de su dirección de IP.

La protección contra los ataques puede, así mismo, ser implementada sobre conmutadores y encaminadores. Una posibilidad es configurar el entorno PVLAN para el aislamiento del nivel 2. Una PVLAN ofrece una subdivisión adicional dentro de una VLAN existente, haciendo posible que los puntos de conexión individuales sean separados de otros compartiendo al tiempo la misma subred de IP. Esto permite que se produzca la separación entre los dispositivos sin que se requiera una subred de IP separada para cada dispositivo. En su forma más simple, las PVLANs soportan puntos de conexión aislados y puntos de conexión promiscuos. Los puntos de conexión aislados pueden únicamente comunicarse con puntos de conexión promiscuos mientras que los puntos de conexión promiscuos pueden comunicarse con cualquier punto de conexión. En este despliegue, los miembros de una subred son puntos de conexión aislados, y el dispositivo de pasarela está conectado a un punto de conexión promiscuo. Esto permite que los anfitriones de una subred no atiendan las solicitudes de los miembros de la misma subred.

Otra posibilidad sería que la característica de la VLAN visitadora privada del estándar 802.1x extendiera una VLAN visitadora del estándar 802.1x hacia el entorno de la PVLAN para el aislamiento del nivel 2. La VLAN visitadora privada del estándar 802.1x ofrece un acceso a red limitado a través de una PVLAN secundaria visitadora a los usuarios sin un suplicante del 802.1x.

Otro procedimiento, bastante directo, sería utilizar una técnica de ACL o simplemente restringir un número mínimo de direcciones de MAC a las VLANs dispuestas sobre un punto de conexión troncal.

La presente invención da soporte a diversas formas de impedir las asociaciones inapropiadas sin intención lesiva. Por ejemplo, cada terminal que se asocia con un SSID de servicio de emergencia debe enviar una TSPEC para requerir la emergencia dentro de un determinado periodo de tiempo, de lo contrario es desasociado y / o preterido por el AP 20. Como alternativa el SSID puede estar oculto y es obligatorio un escaneo activo para asociarlo al SSID de emergencia.

La llamada de servicio de emergencia puede ser priorizada mediante el desencadenamiento del terminal 10 del uso de una especificación de tráfico TSPEC para indicar que el flujo del RTP tiene una prioridad de emergencia de voz. Así mismo, es posible que pueda ser utilizado un procedimiento de desalojo para favorecer una llamada de emergencia con respecto a llamadas de menor prioridad.

Las Figuras 3a a 3c muestran tres ejemplos diferentes relacionados con el encaminamiento de paquetes de una llamada de emergencia. En cada una de las figuras 3a a 3c, se transmite una secuencia de mensajes entre el terminal 10, el punto de acceso 20 de la LAN 3, un servidor 22 de l NAT asociado con el punto de acceso 20, el servidor 30 del DHCP, el gestor de llamadas 40 y el PSAP 60.

La Fig. 3a muestra una secuencia de flujo de mensajes relacionada con un encaminamiento de paquetes en base a un procedimiento del DHCP. Con este procedimiento del DHCP un cliente pide – al solicitar una dirección de IP – una opción concreta del DHCP que proporcione al cliente la dirección de IP del gestor de llamadas. En una primera etapa del procedimiento, el terminal 10 envía un mensaje 210 DHCP DISCOVER. Para que el terminal 10 sea capaz de utilizar el servidor 30 del DHCP, ambos servicios deben estar situados dentro de la misma red de IP a menos que se utilice un retransmisor del DHCP. Si ambos dispositivos no están dentro de la misma red de IP, puede ser utilizado un dispositivo de asistencia del DHCP, como por ejemplo una unidad de retransmisión del DHCP o una unidad de ayuda del DHCP la cual retransmita y / o reenvíe los mensajes relacionados con el DHCP hacia la red en la que el servidor del DHCP está situado.

El mensaje 210 DHCP DISCOVER enviado por el terminal 10 llega al servidor 30 del DHCP. Esto puede conseguirse mediante el envío del mensaje 210 DHCP DISCOVER en radiodifusión si el terminal 10 y el servidor 30 del DHCP están en la misma red, por ejemplo una VLAN, o a través de un ayudante del DHCP. Por medio del mensaje 210 DHCP DISCOVER, el terminal 10 solicita una dirección de IP del servidor 30 del DHCP. De modo preferente, el mensaje 210 DHCP DISCOVER comprende una dirección de MAC del terminal 10 (MAC = Control de Acceso al Medio {[Media Access Control}]). La dirección de MAC, conocida también como dirección LAN, ID de Ethernet o ID de aeropuerto, es la dirección hardware de un dispositivo de red la cual sirve para la identificación única del dispositivo existente en la red.

De modo preferente, el terminal 10 envía el mensaje 210 DHCP DISCOVER como una retransmisión de red a todos los servidores disponibles del DHCP. Es posible que varios servidores del DHCP estén situados dentro de la misma subred de IP. El mensaje 210 de radiodifusión DHCP DISCOVER puede acarrear como dirección de IP de remitente 0.0.0.0 y puede ser dirigido a la dirección de destino 255.255.255.255, dado que el terminal 10 de envío no posee una dirección de IP, todavía, y dirige la solicitud a todos los servidores alcanzables del DHCP.

El servidor 30 del DHCP recibe el mensaje 210 DCHP DISCOVER y contesta con un mensaje 211 DHCP OFFER el cual comprende una oferta de una dirección de IP para el terminal 10 solicitante. El mensaje 211 DHCP OFFER comprende así mismo un ID del servidor que identifica el servidor 30 remitente del DHCP y una dirección de IP y un punto de conexión del gestor de llamadas 40. Es posible que el terminal 10 reciba más de un mensaje de oferta procedente de servidores del DHCP diferentes. De esta manera, el terminal puede escoger entre las ofertas recibidas. Después de seleccionar una de las una o más ofertas propuestas, el terminal contacta, por medio de un mensaje 212 DHCP REQUEST, con el servidor 30 apropiado del DHCP el cual es identificado por medio del correspondiente ID de servidor. De modo preferente, el mensaje 212 DHCP REQUEST es difundido.

En respuesta, el servidor 30 del DHCP transmite un mensaje 213 DHCP ACK (= acknowledge) al terminal solicitante 10. El mensaje 213 DHCP ACK comprende una dirección de IP del terminal 10, la dirección de IP del gestor de llamadas 40 y un punto de conexión sobre el cual el gestor de llamadas 40 está constantemente escuchando, y los datos adicionales relevantes.

De esta manera, en la etapa 214, el terminal 10 tiene su propia dirección de IP, la dirección de IP del gestor de llamadas 40 y el punto de conexión 0 sobre el cual está escuchando el gestor de llamadas 40. El terminal 10 dirige los paquetes relacionados con la llamada de emergencia con la dirección de destino y con el punto de conexión con el gestor de llamadas 40 y envía los paquetes dirigidos al gestor de llamadas 40. Se establece un flujo 215 del RTP entre el terminal 10 y el gestor de llamadas 40. El gestor de llamadas 40 recibe los paquetes relacionados con la llamada de emergencia, inicia un establecimiento de llamada 216 hacia el PSAP relevante 60 y reenvía los paquetes al SPAP 60.

La Fig. 3b muestra una secuencia de flujo de mensajes relacionados con un encaminamiento de paquetes basado en una NAT de destino. Con este procedimiento de la NAT de destino, un cliente puede enviar paquetes a cualquier dirección de destino una vez que ha recibido una dirección de IP. Un servidor 22 de la NAT modificará esta dirección en una del gestor de llamadas 30. Las etapas 220 a 224 de la Fig. 3b se corresponden con las etapas 210 a 214 mostradas en la Fig. 3a. La única diferencia con respecto al procedimiento ilustrado en la Fig. 3a es que el mensaje 221 DHCP OFFER y el mensaje 223 DHCP ACK no comprenden la dirección de IP y el punto de conexión del gestor de llamadas 40.

Es, así mismo, posible que el terminal 10 reciba una dirección de IP para unirse a la LAN 3 por medio de otro procedimiento distinto del de a través del DHCP.

En la etapa 224, el terminal 10 solo recupera su dirección de IP. El terminal 10 dirige los paquetes relacionados con la llamada de emergencia con cualquier dirección de IP como dirección de destino y envía los paquetes dirigidos al servidor 22 de la NAT asociado con el AP 20. Se establece un flujo 225 del RTP entre el terminal 10 y el servidor 22 de la NAT. El servidor 22 de la NAT recibe los paquetes procedentes del terminal 10 y traduce la dirección de destino a la dirección de IP del gestor de llamadas 40. Se establece un flujo 226 del RTP entre el servidor 22 de la NAT y el gestor de llamadas 40. El gestor de llamadas 40 recibe la información relacionada con la llamada de emergencia en forma de paquete o en forma de flujo, inicia un establecimiento de llamada 227 hacia el PSAP relevante 60 y reenvía los paquetes al PSAP 60.

La Fig. 3c muestra una secuencia de flujo de mensajes relacionada con un encaminamiento de paquetes en base a un procedimiento de multidifusión. Con este procedimiento de multidifusión, un cliente – una vez que ha recibido una dirección de IP – envía los paquetes a una dirección de multidifusión bien conocida situada en un punto de conexión predefinido sobre el cual el gestor de llamadas 40 está escuchando. Las etapas 230 a 234 de la Fig. 3c se corresponden con las etapas 210 a 214 mostradas en la Fig. 3a. La única diferencia con respecto al procedimiento ilustrado en la Fig. 3a es que el mensaje 231 DHCP OFFER y el mensaje 233 DHCP ACK no comprenden la dirección de IP y el punto de conexión del gestor de llamadas 40.

Es, así mismo, posible que el terminal 10 reciba una dirección de IP para unirse a la LAN 3 por medio de otro procedimiento distinto del de a través del DHCP.

En la etapa 234, el terminal 10 solo recupera su dirección de IP. El terminal 10 dirige los paquetes relacionados con la llamada de emergencia con una dirección de IP de multidifusión como dirección de destino y envía los paquetes dirigidos al gestor de llamadas 40. Se establece un flujo 235 del RTP entre el terminal 10 y el gestor de llamadas 40. El gestor de llamadas 40 recibe la información (en forma de paquete / flujo) relacionada con la llamada de emergencia, inicia un establecimiento de llamada 236 hacia el PSAP relevante 60 y reenvía los paquetes al PSAP 60.

La Figura 4 muestra un grupo 700 de usuarios autorizados de la WLAN 2 que comprende los terminales 70 a 73. El grupo 700 de usuarios autorizados es capaz de acceder a la LAN 3 con una llamada no de emergencia mediante la utilización de un primer SSID 7. Al mismo tiempo los miembros del grupo 700 son también miembros de un grupo abierto 800. El grupo abierto 800 comprende tanto los usuarios autorizados de los terminales 70 a 73 como los usuarios no autorizados de la WLAN 2 con los terminales 10 a 13. Solo el grupo 700 de usuarios autorizados está legitimado para acceder a la LAN 3 con una llamada de no emergencia utilizando un primer SSID 7. Sin embargo, tanto los miembros del grupo 700 como los miembros del grupo 800 están habilitados para acceder a la LAN 3 con una llamada de emergencia mediante la utilización de un SSID de emergencia 8, dado que el grupo 800 está situado dentro del área de cobertura del punto de acceso 20. Cualquier terminal del grupo 700 o del grupo 800 puede acceder a la LAN 3 por medio del punto de acceso 20 utilizando el SSID de emergencia 8, por ejemplo, el terminal 10 o el terminal 71.

Por consiguiente, cualquier terminal del área de cobertura o del punto de acceso 20 puede acceder a la LAN 3 en caso de una emergencia mediante la utilización del SSID de emergencia 8. En el caso de una llamada no de emergencia, solo los terminales del grupo autorizado 700 que comprende los usuarios autorizados de la WLAN 2 pueden acceder a la LAN 3 por medio del punto de acceso 20. Aunque las llamadas asociadas con el SSID de emergencia 8 serán encaminadas hacia el PSAP 60, una llamada no de emergencia, por ejemplo originada en el terminal 70, puede ser encaminada hacia otro asociado 90 de la comunicación en un procedimiento, tal y como es conocido en la técnica anterior.

Con el fin de imponer el control de acceso, la función 21 de control de acceso puede – además de restringir el acceso a la LAN 3 a los paquetes de datos procedentes de un terminal asociado con un SSID autorizado – aplicar reglas adicionales a los paquetes de datos entrantes. Es posible que cada usuario que envía paquetes de datos desde un terminal asociado con un SSID de emergencia hacia la LAN 2 pueda tener asignado un ancho de banda limitado que sea suficiente para establecer la llamada de emergencia con el PSAP 60 pero que no sea lo suficientemente ancho para establecer otras llamadas. Este mecanismo de control de acceso puede funcionar dado que una llamada de emergencia puede estar más bien restringida con respecto a la cantidad de datos.

Estrechamente relacionada con este mecanismo de control de acceso es la técnica de admitir solo tráfico de voz en la LAN 3. De esta manera, los paquetes de datos relacionados con aplicaciones que consumen ancho de banda como vídeo, son rechazados por la LAN 3 si los paquetes de datos intentan entrar en la LAN 3 mediante la utilización de un SSID de emergencia.

La Figura 5 muestra una red 400 para la transmisión de paquetes de IP y dos redes de acceso inalámbricas 401, 402 para proporcionar acceso a la red 400. La red de acceso corporativo 401 es una red de acceso corporativo solo accesible mediante terminales de usuario autorizados 701, 702, mientras que la red de acceso de emergencia 402 es accesible para fines de emergencia por cualquier terminal de usuario móvil dentro del área de servicio de la red de acceso de emergencia 402, esto es, tanto por los terminales de usuario autorizados 701, 702 como por los terminales de usuario visitadores 801 a 803.

Los terminales autorizados 701, 702 pueden comprender unos módulos de encriptación 7010, 7020 que permitan que los terminales 701, 702 encripten de manera apropiada paquetes de datos antes de transmitirlos a la red de acceso 4012.

Cada red de acceso 401, 402 difunde, por medio de un remitente, por ejemplo por medio de un AP, un SSID específico a la red de acceso respectiva. La red de acceso corporativa 401 difunde un SSID corporativo asociado con la red de acceso corporativo 401, y la red de acceso de emergencia 402 difunde un SSID de emergencia asociado con la red de acceso de emergencia 401. Los SSIDs difundidos pueden ser recibidos por cualquier terminal existentes en el área de cobertura de las redes de acceso 401, 402.

La red de acceso corporativa 401 comprende una función 4011 de control de acceso y, de manera similar, la red de acceso de emergencia 402 comprende una función 4021 de control de acceso. Las funciones 4011, 4012 de control de acceso son implementadas como servidores autónomos que comprenden unas normas de control de acceso almacenadas en un módulo de memoria. Cada una de las funciones 4011,4021 de control de acceso filtra los paquetes de datos entrante antes de admitirlos en las redes de acceso 401, 402.

Los paquetes de datos procedentes de un terminal asociado con el SSID de emergencia asociado con la red de acceso de emergencia 402 tienen un acceso garantizado por la función 4021 de control de acceso a la red de acceso de emergencia 402. Solo los terminales de usuario autorizados 701, 702 pueden ser capaces de encriptar de manera adecuada paquetes de datos por medio de los módulos de encriptación 7010, 7020. Los paquetes de datos

que llegan a la función 4011 de control de acceso deben proceder de un terminal asociado con el correspondiente SSID corporativo asociado con la red de acceso corporativa 401 y pueden ser encriptados de manera adecuada para ser admitidos en la red de acceso 401. Por medio de una técnica de encriptación, la función 4011 de control de acceso filtra los paquetes de dato entrantes y descarta los paquetes de datos que no proceden de terminales de usuario autorizados. La función 4011 de control de acceso recupera los datos relevantes para el proceso de filtrado y examen a partir de una base de datos 4012.

El terminal de usuario visitador 801 ha tomado nota del SSID corporativo y utiliza el SSID corporativo para acceder a la red de acceso corporativa 401. Es posible que un administrador de la red de red de acceso corporativo 401 configure un SSID corporativo público que se establezca sobre un punto de acceso de la red de acceso corporativa 401 difundida a todos los dispositivos inalámbricos en cobertura. De esta manera, la SSID corporativa ha sido difundida abiertamente por la red de acceso corporativa 401 y el terminal de usuario visitador 801 ha recibido el SSID corporativo recogiendo el SSID corporativo difundido.

Sin embargo, también es posible que el terminal 801 de usuario visitador esté asociado con un escuchón el cual quiere utilizar los servicios de comunicaciones ofrecidos por la red de acceso corporativa 401 de una forma no autorizada. Imaginemos que el administrador de la red de la red de acceso corporativo 401 ha inhabilitado el elemento característico de difusión automática del SSID en una tentativa por mejorar la seguridad de la red cuando la difusión pública del SSID corporativo puede plantear un riesgo para la seguridad. Sin embargo, la protección ofrecida por la desactivación de una difusión de la SSID puede ser fácilmente sorteada por el escuchón en cuanto el SSID puede ser rastreada en texto no cifrado a partir de un paquete de datos enviado por un terminal autorizado 701, 702 a la red de acceso corporativa 401.

Sin embargo, el terminal de usuario visitador 801 que ha recibido el SSID corporativo, se asocia con el SSID corporativa y envía un flujo 301 de paquetes de datos a la red de acceso corporativa 401. Cuando el terminal 801 del usuario visitador carece de medios para encriptar de forma adecuada los paquetes de datos 301, el examen desarrollado por la función 4011 de control de acceso sobre el flujo 301 de paquetes de datos se traduce en un rechazo de paquetes de datos.

Por otro lado, el terminal 701 del usuario autorizado que comprende el módulo de encriptación 7010 envía unos paquetes de datos 1001 a la red de acceso corporativa 401, los cuales están dispuestos de forma que proceden de un terminal asociado de la SSID corporativa así como están adecuadamente encriptados. De esta manera, el proceso de examen en la función 4011 de control de acceso se traduce en la admisión a la red de acceso. Así mismo, los paquetes de datos 1002 procedentes del otro terminal 702 del usuario autorizado son, así mismo, admitidos en la red de acceso corporativa 401.

Cuando el terminal 702 del usuario autorizado envía los paquetes de datos 502 desde un terminal asociado con el SSID de emergencia a la función 4021 de control de acceso, los paquetes de datos 502 son emitidos en la red de acceso de emergencia 402. El terminal 802 del usuario visitador envía un flujo 501 de paquetes de datos relacionado con el SSID de emergencia hacia la red de acceso corporativa 401 pero no es admitido en la red de acceso corporativa 401, dado que el flujo 501 de paquetes de datos ni procede de un terminal asociado con el SSID apropiado ni está encriptado de forma apropiada. Sin embargo, cuando el terminal 802 del usuario visitador asociado con el SSID de emergencia envía un flujo 502 de paquetes de datos hacia la red de acceso de emergencia 402, el flujo 502 de paquetes de datos es admitido en la red de acceso de emergencia 402 por la función 4021 de control de acceso dado que los paquetes de datos 503 proceden de un terminal asociado con el SSID de emergencia.

Cuando el terminal 803 del usuario visitador asociado con el SSID corporativo envía los paquetes de datos 302 a la red de acceso de emergencia 402, el flujo 302 de paquetes de datos es rechazado por la función 4021 de control de acceso. La función 4021 de control de acceso solo admite paquetes de datos procedentes de un terminal asociado con el SSID de emergencia.

Después de entrar en la red de acceso corporativa 401, los flujos de datos 1001 y 1002 son reenviados como flujos de datos 601 y 602 a la red 400 y encaminados hacia un elemento de red 4001, por ejemplo un encaminador o un conmutador, el cual encamina o conmuta los flujos de datos 601 y 602 de acuerdo con las direcciones de destino de ID indicadas en los paquetes de datos de los flujos de datos 601 y 602.

Por ejemplo, cuando el usuario del terminal 701 del usuario autorizado marca el número de teléfono VoIP de un copartícipe de comunicación corporativo, un agente usuario del VoIP del terminal 701 del usuario autorizado dirige en la medida correspondiente los paquetes de datos 1001, 601 con la dirección correspondiente, y el flujo 601 de los paquetes de datos es encaminado por el elemento de red 4001 hacia otro elemento de red 4002 el cual es responsable de la dirección. El establecimiento de una conexión requiere un intercambio de mensajes de señalización y control para el encaminamiento apropiado y el establecimiento de la llamada. Así mismo, los paquetes de datos 1002 son encaminados a través del elemento de red 4002 hacia otro elemento de red 4003. No hay ningún encaminamiento preestablecido, sino que cada salto siguiente en la red 400 se determina por cada elemento de red, de forma individual, para cada paquete de datos de acuerdo con la dirección indicada de un paquete de datos.

Por otro lado, los flujos de datos 502, 503 que llegan y son admitidos en la red de acceso de emergencia 402 son encaminados a un gestor de llamadas 4001, por ejemplo, una PBX, la cual encamina los paquetes de datos hacia un punto contestador 60 de servicios de emergencia, por ejemplo un PASP (PBX = Centralita [Private Branch Exchange]). El encaminamiento es ejecutado sobre una conexión sin necesidad de ningún tráfico de señalización y control.

Así mismo, es posible que, con independencia de la dirección efectiva del paquete de datos, la dirección de destino original del paquete de datos admitidos en la red de acceso de emergencia de la red 402 puede ser eliminado de los paquetes de datos sustituidos por una dirección estándar preestablecida asociada con el servicio de emergencia, por ejemplo, una red de IP y un punto de conexión del gestor de llamadas 4001. Mediante este sistema estandarizado y preestablecido, resulta posible una respuesta de las llamadas de emergencia rápida y fiable.

Las Figuras 6a a 6d muestran cuatro ejemplos diferentes relacionados con la localización de un terminal que inicia una llamada de emergencia. En cada una de las Figuras 6a a 6d, una secuencia de mensajes es transmitida entre el terminal 10, el punto de acceso 20 de la LAN 3, el servidor 30 del DHCP, un servidor de localización 35, el gestor de llamadas 40 y el PSAP 60. El servidor de localización 35 alberga unos servicios web que proporcionan la transmisión de la información de localización al PSAP.

La Fig. 6a muestra una secuencia de flujo de mensajes determinada por la localización del terminal 10 de acuerdo con una primera alternativa. En una primera etapa del procedimiento, el terminal 10 después de la asociación con una SSID de emergencia, envía un mensaje 510 de difusión activa a través del AP 20 al servidor de localización 35 (SOAP = Protocolo de Acceso de Objetos Simples [Simple Object Access Protocol]). El mensaje 510 de difusión activa del SOAP comprende una información de localización del terminal 10, por ejemplo un BSSID del AP 10 a través del cual el terminal tiene acceso a la VLAN (BSSID = Identificador de Conjuntos de Servicios Básicos [Basic Service Set Identifier]). El BSSID es un identificadr único de un AP en una LAN. La especificación de la LAN Inalámbrica del estándar 802.11 1999 del ZEGE define un BSSID como una dirección de MAC que identifica una estación (STA) de un AP en un modo de infraestructura. De esta manera, el BSSID identifica de forma unívoca cada AP lo cual es indispensable para distinguir los APs con un SSID idéntico.

El servidor de localización 35 responde una contestación 511 la cual actúa como una confirmación de la solicitud 510. Si el terminal 10 no recibe ninguna respuesta dentro de un periodo de tiempo determinado después del envío del mensaje 510 de solicitud del SOAP, el terminal 10 puede reenviar el mensaje 510 de solicitud del SOAP.

Tan pronto como el gestor de llamadas 40 advierte una llamada de emergencia, el gestor de llamadas comienza a sondear de forma regular el servidor de localización 35 mediante el envío de un mensaje de sondeo 512 al servidor 35. El mensaje de sondeo 512 provoca que el servidor de localización 35 informe al gestor de llamadas 40 de cualquier información de actualización relacionada con la información de localización del terminal 10. El servidor de localización 35 siempre responde con una información de localización. El servidor de localización 35 responde al mensaje de sondeo 512 mediante el envío de una respuesta 513. La respuesta 513 comprende, o bien una información de actualización relativa a la localización del terminal, o bien una indicación de que no se encuentra disponible ninguna actualización de localización. El gestor de llamadas 40 simplemente reenviará la información de localización recuperada en forma de mensaje 514 al PSAP 60 o procesará la información de localización recuperada y, a continuación, enviará la información de localización procesada en forma de mensaje 514 al PSAP 60.

Por ejemplo, el servidor de localización 35 puede traducir el BSSID del AP de la información de localización a coordenadas de geográficas, por ejemplo en forma de una base de datos que comprenda los BSSIDs y las correspondientes localizaciones de los APs de la LAN. El gestor de llamadas enviará entonces las coordenadas geográficas al PSAP 60 donde una asistencia será enviada a la localización geográfica indicada.

La Fig. 6b muestra una secuencia de flujo de mensajes relacionada con la localización del terminal 10 de acuerdo con una segunda alternativa. Las etapas 520 a 521 se corresponden con las etapas 510 a 511 descritas con referencia a la Fig. 6a. La descripción correspondiente ofrecida con anterioridad se aplica, así mismo, a la Fig. 6b.

Después de que el servidor de localizaci`´on 35 ha recibido la información de localización o una actualización de la información de localización desde el terminal 10 y, de modo preferente, ha enviado una respuesta 521 al terminal 10, el servidor de localización 35 difunde de forma activa la información de localización hacia el gestor de llamadas 40 por medio del mensaje 522. En respuesta al mensaje 522, el gestor de llamadas 40 envía un mensaje de respuesta 523 de confirmación al servidor de localizador 35.

El gestor de llamadas 40 simplemente reenviará la información de localización recuperada al PSAP 60 en forma de mensaje 524 o procesará la información de localización recuperada y a continuación, enviará la información de localización procesada en forma de mensaje 524 al PSAP 60, de acuerdo con lo descrito con anterioridad con referencia a la Fig. 6a.

La Fig. 6c muestra una secuencia de flujo de mensajes relacionada con la localización del terminal 10 de acuerdo con una tercera alternativa. En una primera etapa del procedimiento el terminal 10, después de su asociación con un SSID de emergencia, envía un mensaje 530 de solicitud de SOAP a través del AP 20 al gestor de llamadas 40. El

mensaje 510 de solicitud de SOAP comprende la información de localización del terminal 10, por ejemplo, un BSSID del AP 10 a través del cual el terminal tiene acceso a la LAN.

El gestor de llamadas 40 responde con una contestación 531 la cual actúa como confirmación de la solicitud 530. Si el terminal 10 no recibe ninguna respuesta dentro de un periodo de tiempo determinado después del envío del mensaje 530 de la solicitud de SOAP, el terminal 10 puede reenviar el mensaje 530 de solicitud de SOAP al gestor de llamadas 40.

Después de que el gestor de llamadas 40 ha recibido la información de localización o una actualización de la información de localización desde el terminal 10 y, de modo preferente, haya enviado una respuesta 531 al terminal 10, el gestor de llamadas 40 simplemente reenviará la información de localización recuperada a modo de mensaje 532 al PSAP 60 o procesará la información de localización recuperada, y a continuación, enviará la información de localización presentada en forma de mensaje 532 al PASP 60,de acuerdo con lo descrito con anterioridad con referencia a la Fig. 6a.

La Fig. 6d muestra una secuencia de flujo de mensajes relacionada con la localización del terminal 10 de acuerdo con una cuarta alternativa. En una primera etapa del procedimiento, el terminal 10, después de su asociación con un SSID de emergencia, envía una solicitud 540 de renovación de DHCP al servidor 30 de DHCP. La solicitud 540 de renovación de DHCP comprende la información de localización del terminal 10, por ejemplo un BSSID del AP 10 a través del cual el terminal tiene acceso a la LAN.

Para seguir avanzando en el procedimiento, tenemos dos opciones. El servidor 30 del DHCP o bien envía un mensaje 541 de SOAP al servidor de localización 35 o envía un mensaje 546 de SOAP al gestor de llamadas 40.

En el primer caso, la información de localización puede ser transmitida al gestor de llamadas 40 o bien mediante un, de modo preferente regular, mensaje de sondeo 542 procedente del gestor de llamadas y la contestación correspondiente 543 procedente del servidor de localización 35, de acuerdo con lo descrito con anterioridad, o mediante la difusión de forma activa de la información de localización por medio de un mensaje 544 procedente del servidor de localización 35 hacia el gestor de llamadas 40 tan pronto como el servidor de localización 35 ha recibido el mensaje 541 de SOAP. De nuevo aquí, el gestor de llamadas 40 puede responder al mensaje 544 con una contestación de confirmación 545.

Después de que el gestor de llamadas 40 ha recibido la información de localización procedente del servidor de localización 35, el gestor de llamadas 40 simplemente reenviará la información de localización recuperada en forma de mensaje 547 al PSAP 60 o procesará la información de localización recuperada y, a continuación, enviará la información de localización procesada en forma de mensaje 547 al PSAP 60, de acuerdo con lo descrito con anterioridad con referencia a la Fig. 6a.

En este último caso, cuando el servidor 30 del DHCP envíe el mensaje 546 de SOAP directamente hacia el gestor de llamadas 40, el gestor de llamadas 40 reenviará de nuevo la información de localización original recuperada o una información de localización procesada en forma de mensaje 547 al PSAP 60.

REIVINDICACIONES

1.- Un procedimiento de provisión a un terminal (10) de un acceso de emergencia sobre una WLAN (2) a una LAN (3) que comprende uno o más puntos de acceso (20) y una función (21) de control de acceso la cual admite paquetes de datos procedentes de usuarios (70 a 73) de la WLAN (2) asociados con un primer SSID (7) hacia la LAN (3), comprendiendo el procedimiento las etapas de:

la definición de uno o más SSIDs de emergencia (8) dedicados a hacer posible el acceso a una LAN (2) en un caso de emergencia;

el inicio de una llamada de emergencia mediante el envío de paquetes de datos desde un terminal (10) asociados con un SSID (8) de emergencia seleccionado hacia uno de los uno o más puntos de acceso (20), por medio de lo cual los paquetes de datos son dirigidos por el terminal (10) hacia una dirección de destino recibida por el terminal (10) por medio de una respuesta de DHCP;

la admisión, mediante la función (21) de control de acceso, de los paquetes de datos procedentes del terminal (10) asociados con el SSID (8) de emergencia seleccionado hacia la LAN (3); y

el encaminamiento de los paquetes de datos asociados con el SSID (8) de emergencia seleccionada,

después de la admisión en la LAN (3), hacia un punto (60) de contestación de emergencia,

por medio de lo cual

el procedimiento comprende las etapas adicionales de

la solicitud por el terminal (10) de una opción concreta del DHCP que proveerá al terminal (10) de una dirección de IP de un gestor de llamadas (40) responsable para la gestión del establecimiento de una llamada de emergencia hacia el punto (60) de contestación de emergencia y un punto de conexión sobre el cual el gestor de llamadas (40) escucha;

la recepción, por el terminal (10), de la dirección de IP del gestor de llamadas (40) y el punto de conexión sobre el cual el gestor de llamadas (40) escucha por medio del DHCP desde un servidor del DHCP; y

el direccionamiento de los paquetes de datos hacia el terminal (10) asociados con la SSID (8) de emergencia seleccionada con la dirección de IP recibida del gestor de llamadas (40) y el punto de conexión sobre el cual el gestor de llamadas (40) está escuchando.

2.- El procedimiento de acuerdo con la reivindicación 1,

caracterizado porque

el procedimiento comprende las etapas adicionales de:

la asociación de dos o más SSIDs (8) de emergencia con diferentes capacidades, de modo preferente con códecs y entramados diferentes; y

la selección de un SSID (8) de emergencia en base a la información extraída de la difusión de uno o más SSIDs (8) de emergencia.

3.- El procedimiento de acuerdo con cualquiera de las reivindicaciones precedentes

caracterizado porque

el procedimiento comprende la etapa adicional de:

la priorización de la llamada de emergencia mediante la utilización de un procedimiento de especificación del tráfico o de un procedimiento de desalojo.

4,- El procedimiento de acuerdo con cualquiera de las reivindicaciones precedentes,

caracterizado porque

el procedimiento comprende las etapas adicionales de:

la difusión de uno o más SSIDs (8) de emergencia desde al menos uno de los uno o más puntos de acceso (20);

la detección, por el terminal (10), de al menos uno de los uno o más SSIDs (8) de emergencia difundidos;

la selección de un SSID (8) de emergencia a partir del al menos un SSID de emergencia detectado;

la asociación, por el terminal (10), con el SSID (8) de emergencia seleccionado.

5.- El procedimiento de acuerdo con cualquiera de las reivindicaciones precedentes,

caracterizado porque

el procedimiento comprende la etapa adicional de:

la generación de salida, después de la detección del al menos uno de los uno o más SSIDs (8) de emergencia, de una notificación en el terminal (10) para informar a un usuario (100) del terminal (10) que se encuentra disponible un acceso de emergencia en la WLAN (2).

6.- Un sistema de comunicación (1) para proveer a un terminal (10) de un acceso de emergencia sobre una WLAN (2) a una LAN (3) comprendiendo el sistema de comunicación una función (21) de control de acceso la cual admite paquetes de datos procedentes de unos usuarios (70 a 73) de la WLAN (2) asociados con un primer SSID (7) en la LAN (3), en el que el sistema de comunicación comprende una interfaz (202) adaptada para recibir paquetes de datos de un terminal (10) asociados con un SSID (8) de emergencia seleccionado entre el al menos un SSID (8) de emergencia seleccionado, una unidad de control (203) adaptada para reenviar los paquetes de datos recibidos del terminal (10) asociados con el SSID (8) de emergencia seleccionado hacia la función (21) de control de acceso, por medio de lo cual la función (21) de control de acceso admite los paquetes de datos procedentes del terminal (10) asociados con el SSID (8) de emergencia seleccionado en la LAN (3), y en el que el sistema de comunicación está adaptado para encaminar los paquetes de datos desde el terminal (10) asociados con el SSID (8) de emergencia seleccionado, después de su admisión en la LAN (2), hacia un punto (60) contestador de emergencia, por medio de lo cual dichos paquetes de datos acarrean una dirección de destino recibida en el terminal (10) a partir del sistema de comunicación (1) por medio de una respuesta del DHCP, y por medio de lo cual

el sistema de comunicación (1) comprende así mimo un gestor de llamadas (40) responsable de la gestión de una configuración de llamadas de emergencia con respecto al punto (60) de contestación de emergencia, y un servidor (30) del DHCP adaptado para proveer, en respuesta a una solicitud procedente del terminal (10) para una correspondiente opción del DHCP concreta, al terminal (10) de una dirección de IP del gestor de llamadas (40) y un punto de conexión sobre el que el gestor de llamadas (40) está escuchando, por medio del DHCP para dirigir los paquetes de datos situados en el terminal (10) asociados con el SSID (8) de emergencia seleccionados con la dirección de IP recibida del gestor de llamadas (40) y con el punto de conexión sobre el que el gestor de llamadas (40) está escuchando.

7.- Un sistema de comunicación de acuerdo con la reivindicación 6,

caracterizado porque

el sistema de comunicación comprende así mismo un remitente (201) adaptado para difundir uno o más SSIDs (8) de emergencia dedicados a autorizar al terminal (10) a acceder a la LAN (3) en un caso de emergencia.

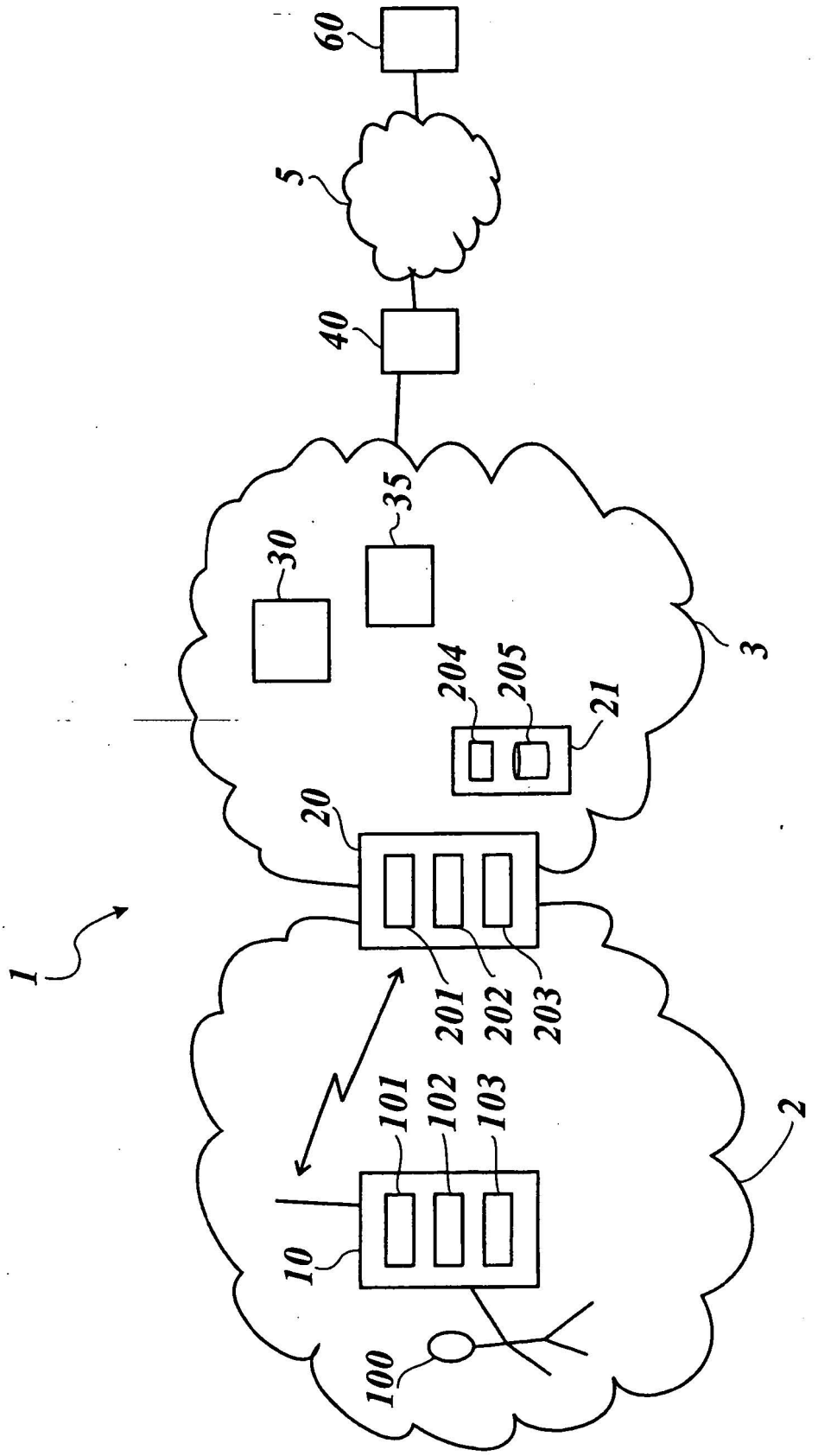

Fig. 1

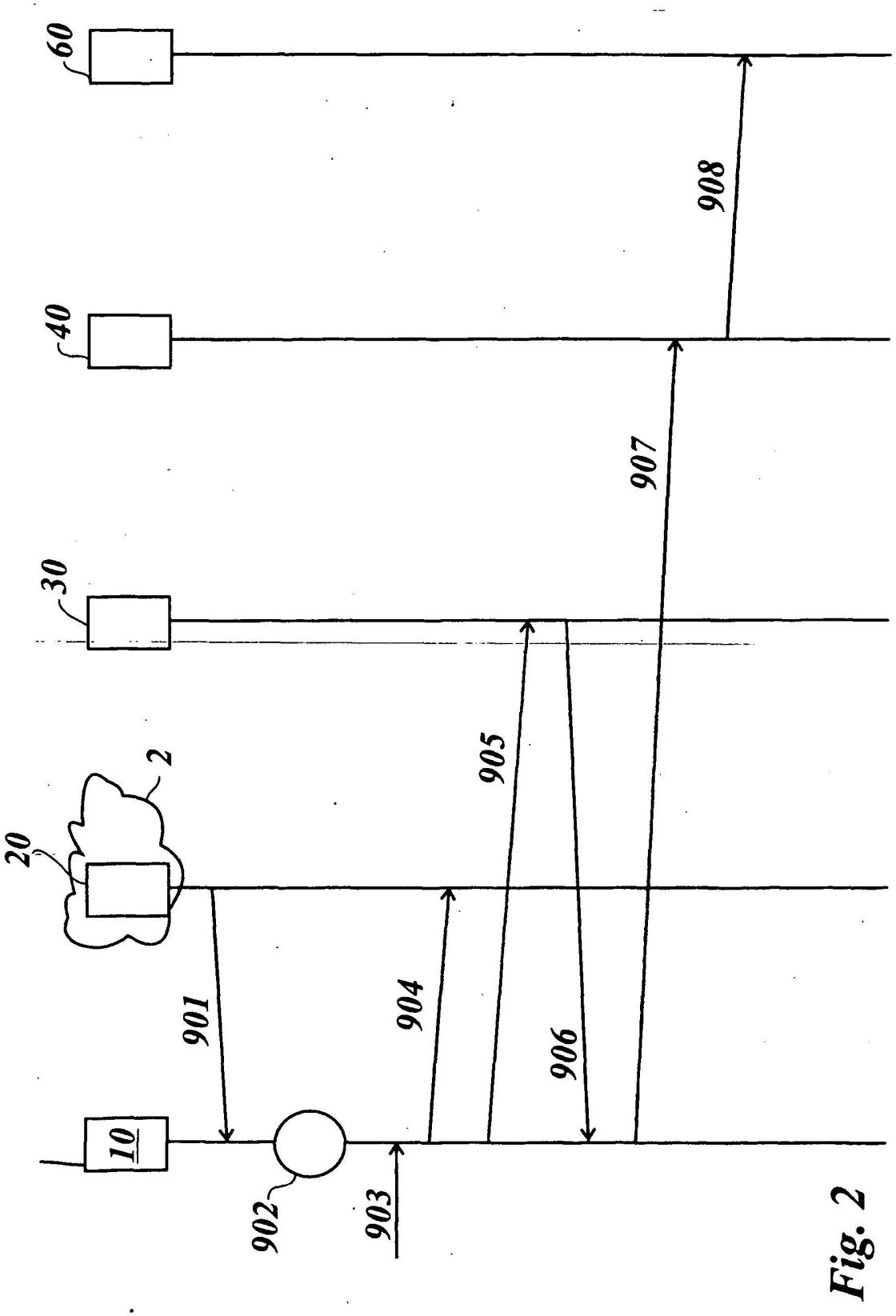

Fig. 2

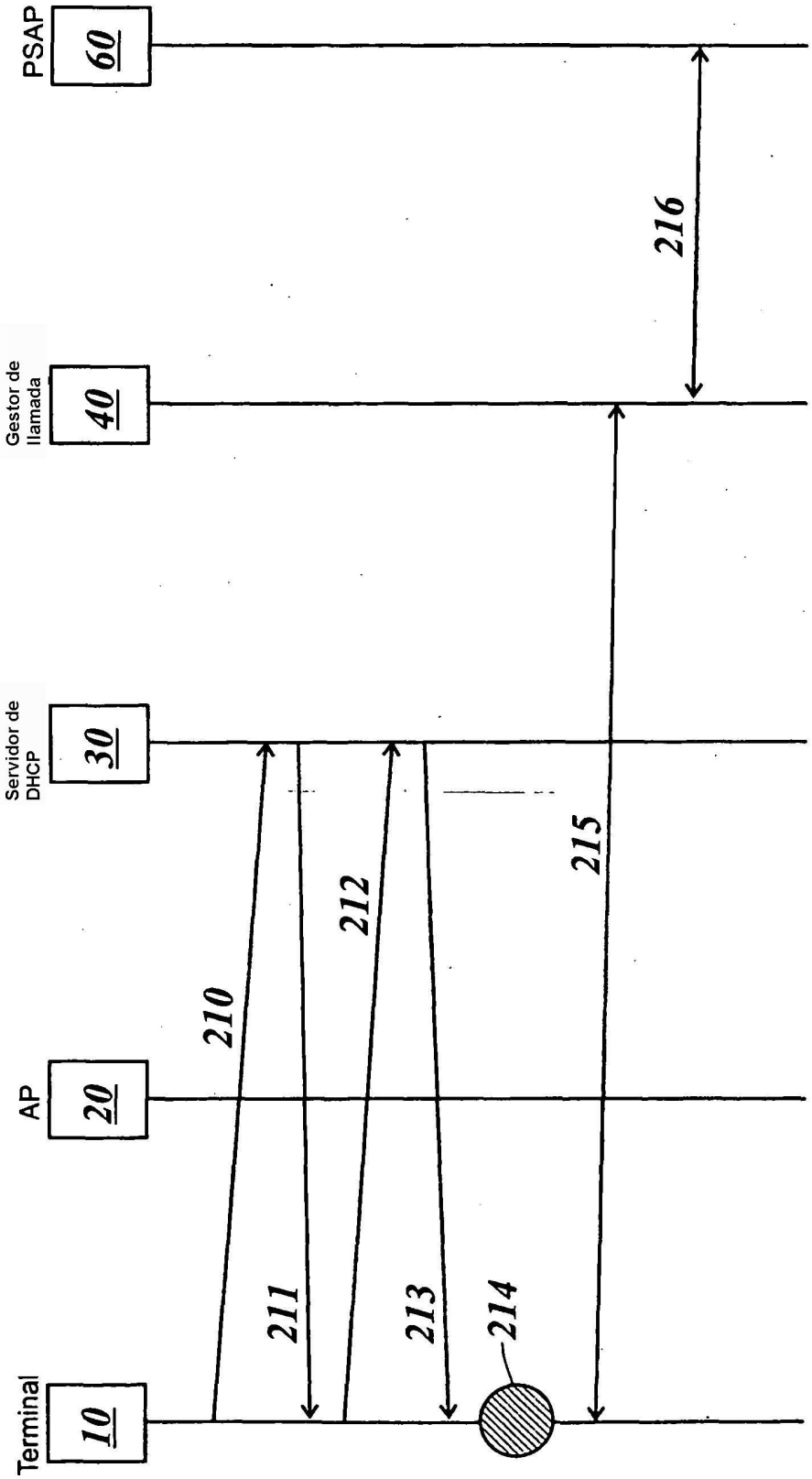
PSAP
60
Gestor de llamada
40
Servidor de DHCP
30
AP
20
Terminal
10
210
211
212
213
214
215
216

Fig. 3a

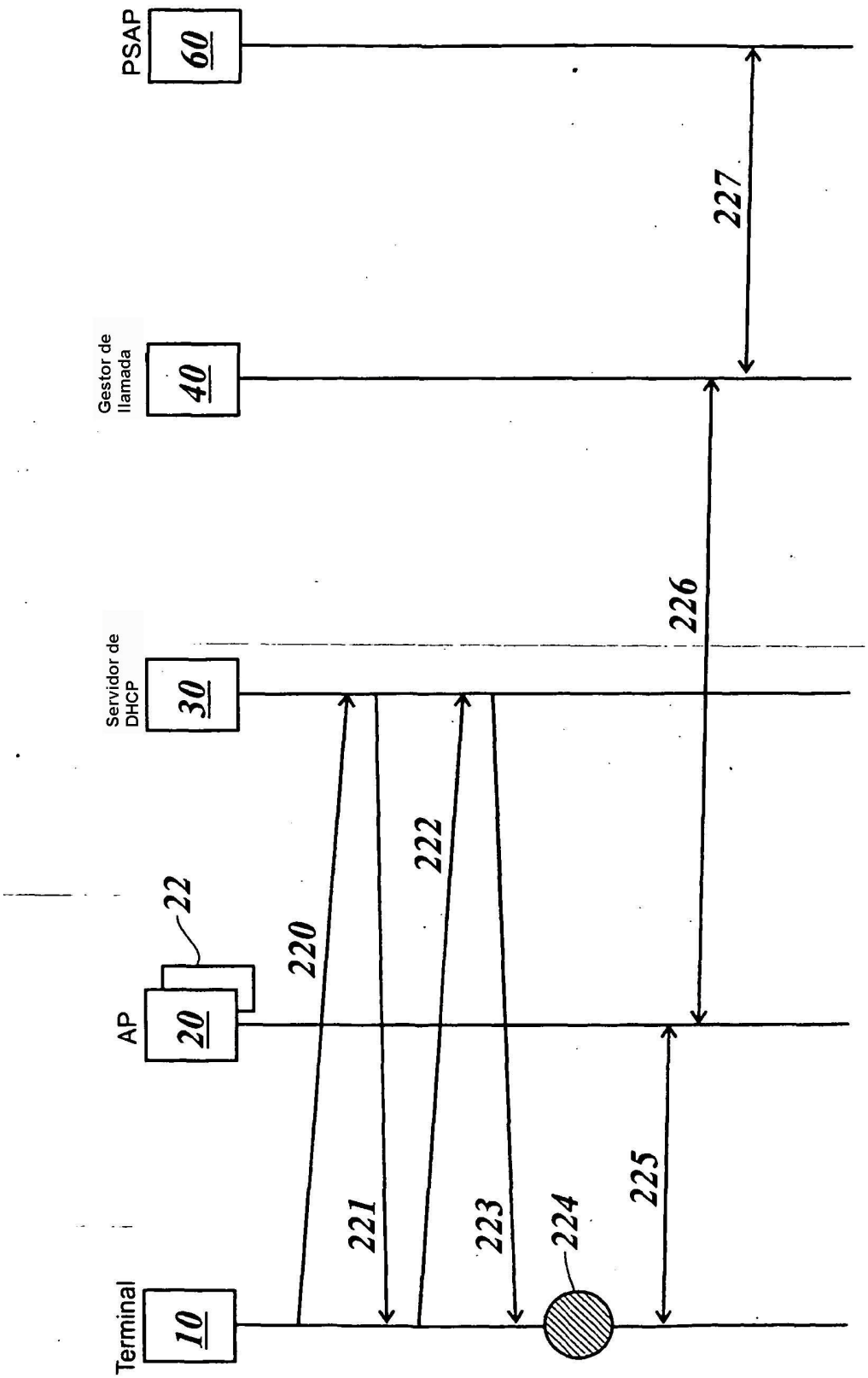
PSAP
60
Gestor de llamada
40
Servidor de DHCP
30
AP
20
22
Terminal
10
220
221
222
223
224
225
226
227

Fig. 3b

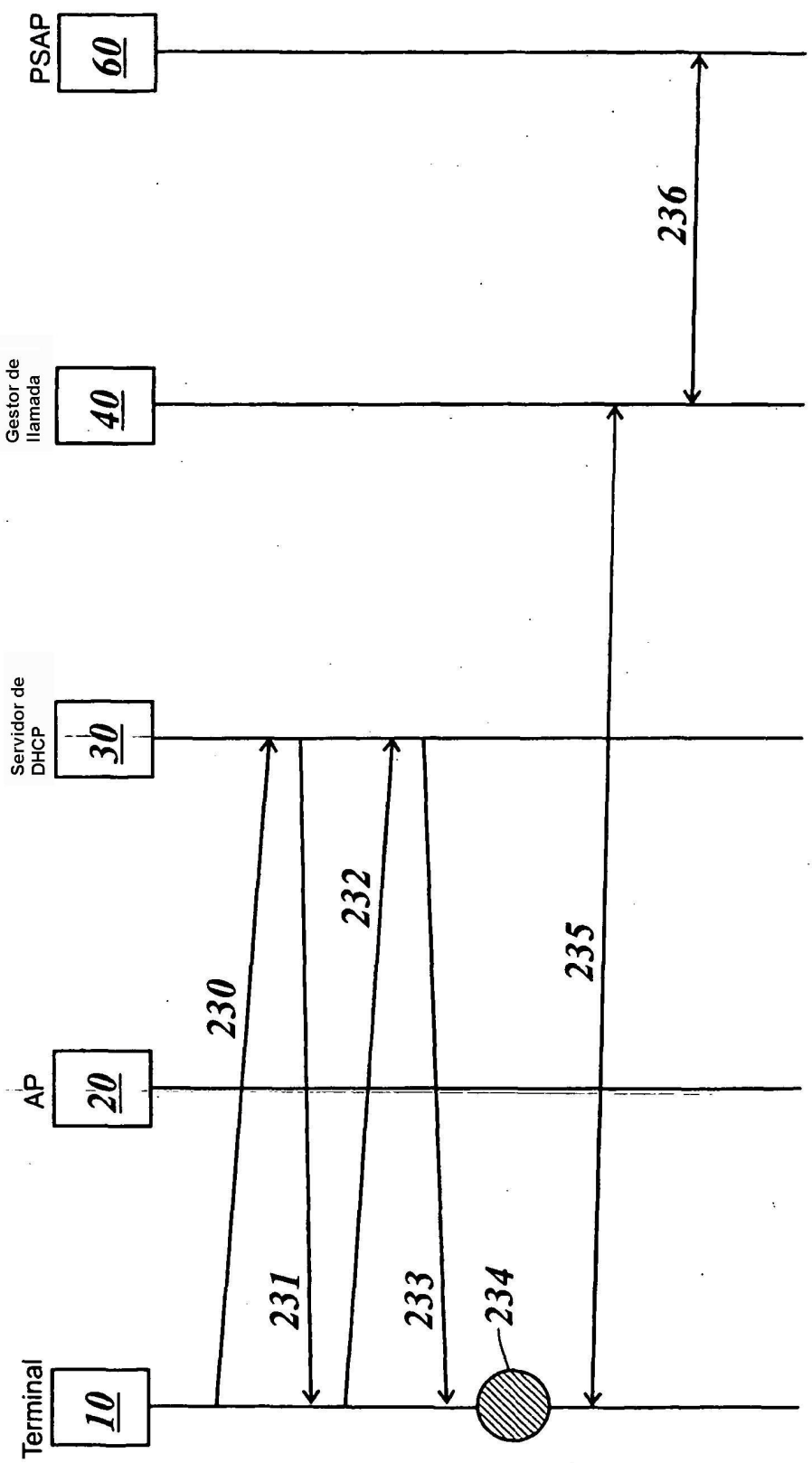
PSAP
60
Gestor de llamada
40
Servidor de DHCP
30
AP
20
Terminal
10
230
231
232
233
234
235
236

Fig. 3c

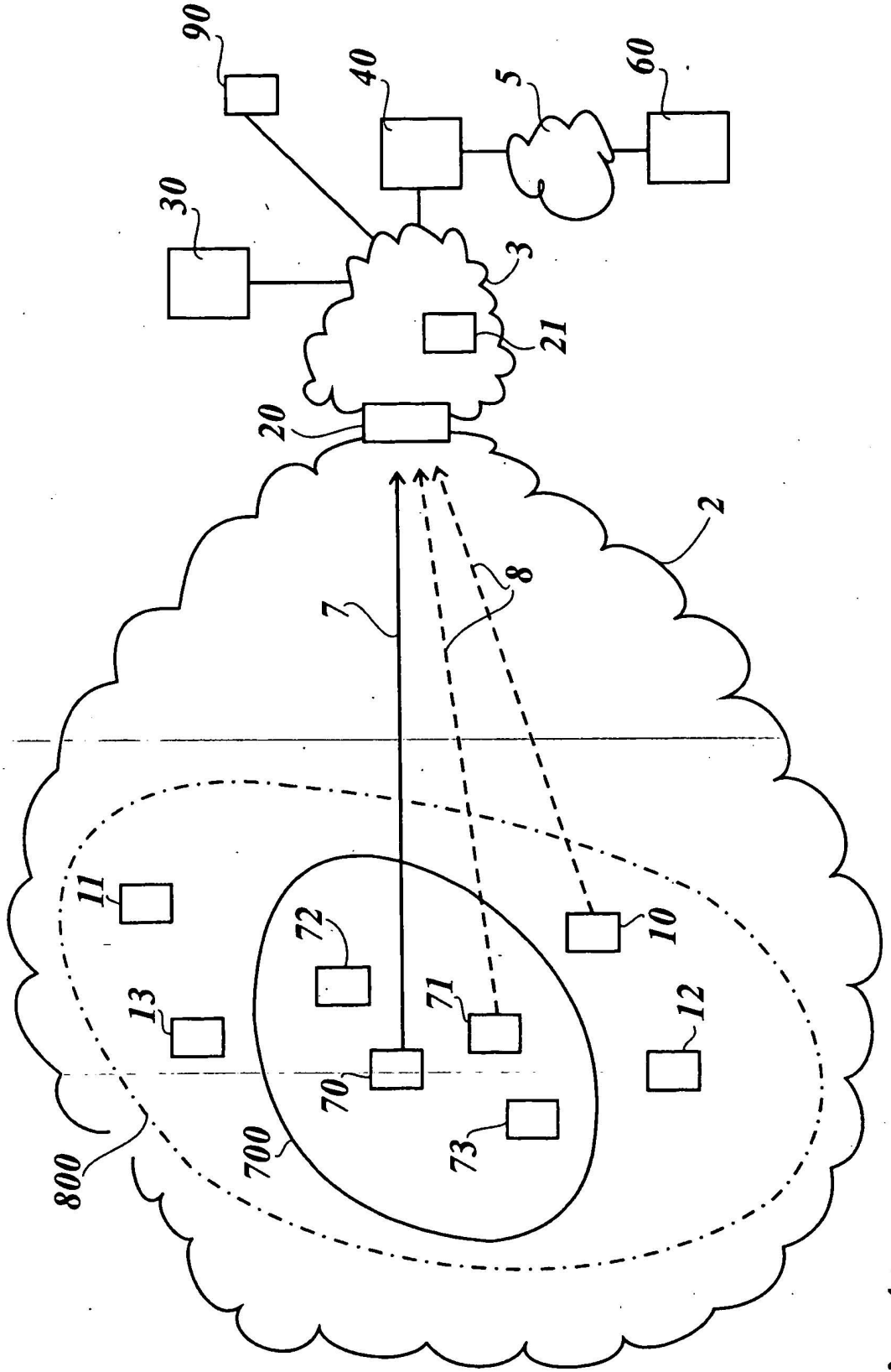

Fig. 4

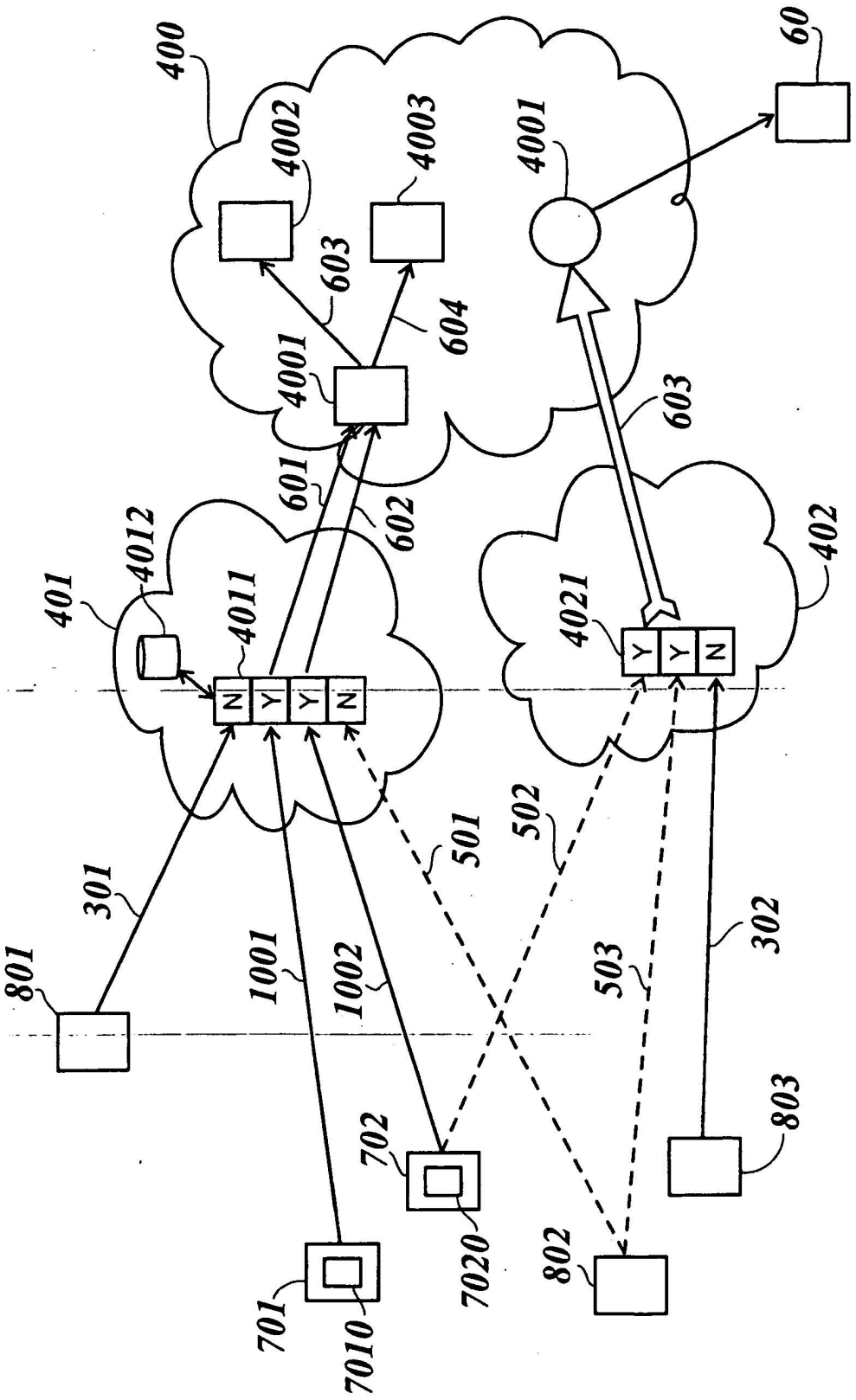
400
4002
4003
4001
60
603
604
4001
601
602
603
4012
401
4011
402
4021
N
Y
Y
N
Y
Y
N
501
502
301
1001
1002
503
302
801
702
803
7020
802
701
7010

Fig. 5

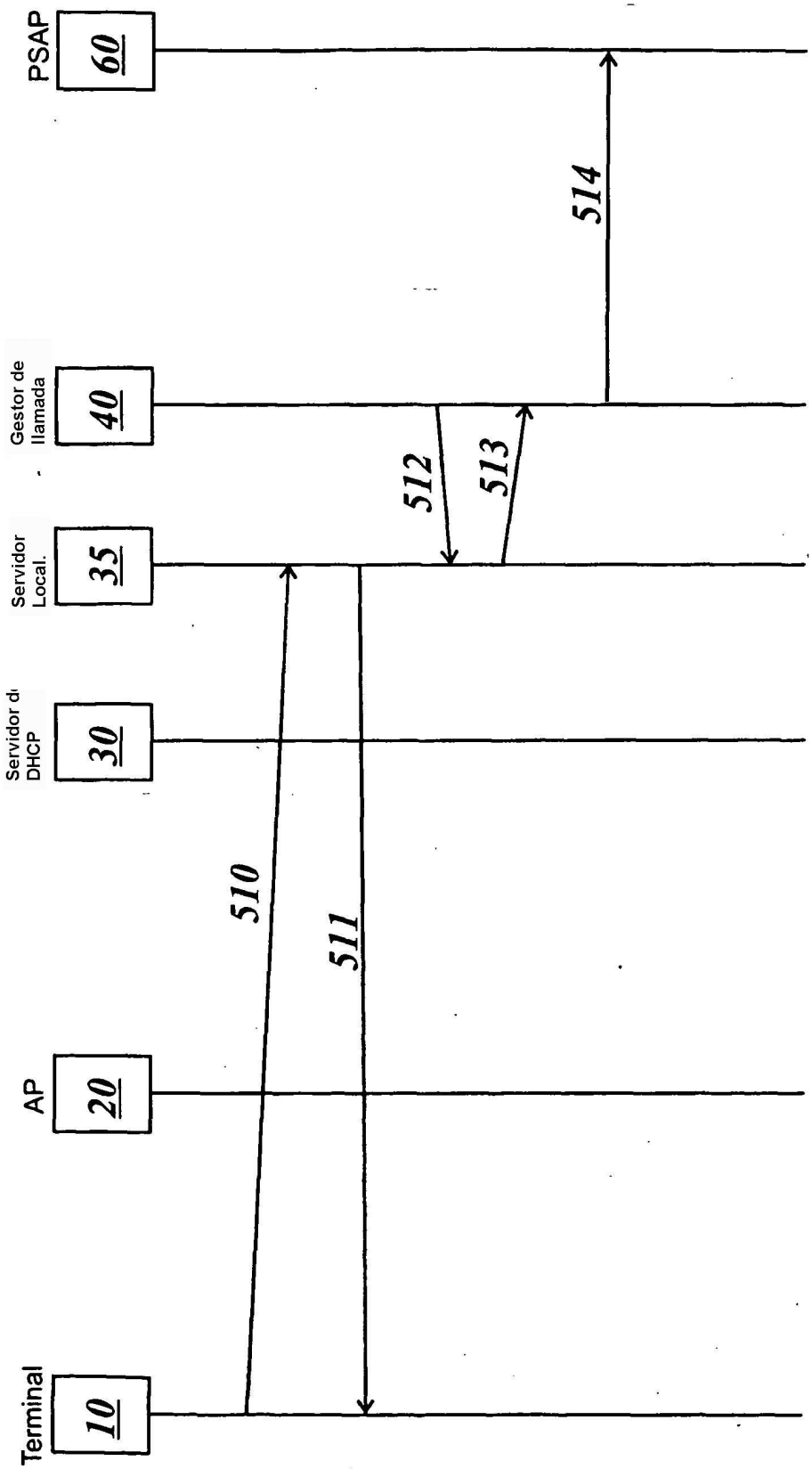
PSAP
60
514
Gestor de llamada
40
512
513
Servidor Local.
35
Servidor d DHCP
30
510
511
AP
20
Terminal
10

Fig. 6a

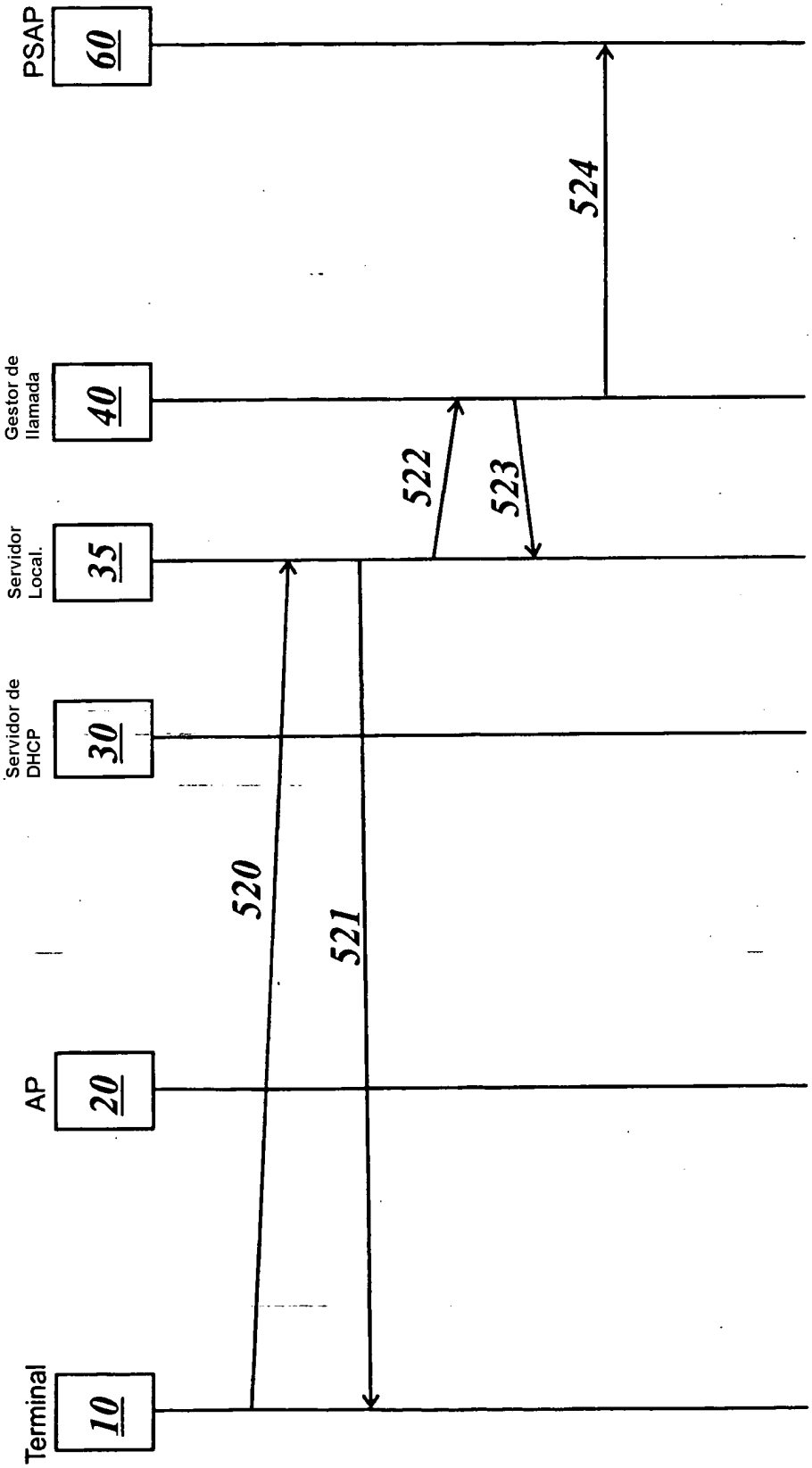
PSAP
60
524
Gestor de llamada
40
522
523
Servidor Local.
35
Servidor de DHCP
30
520
521
AP
20
Terminal
10

Fig. 6b

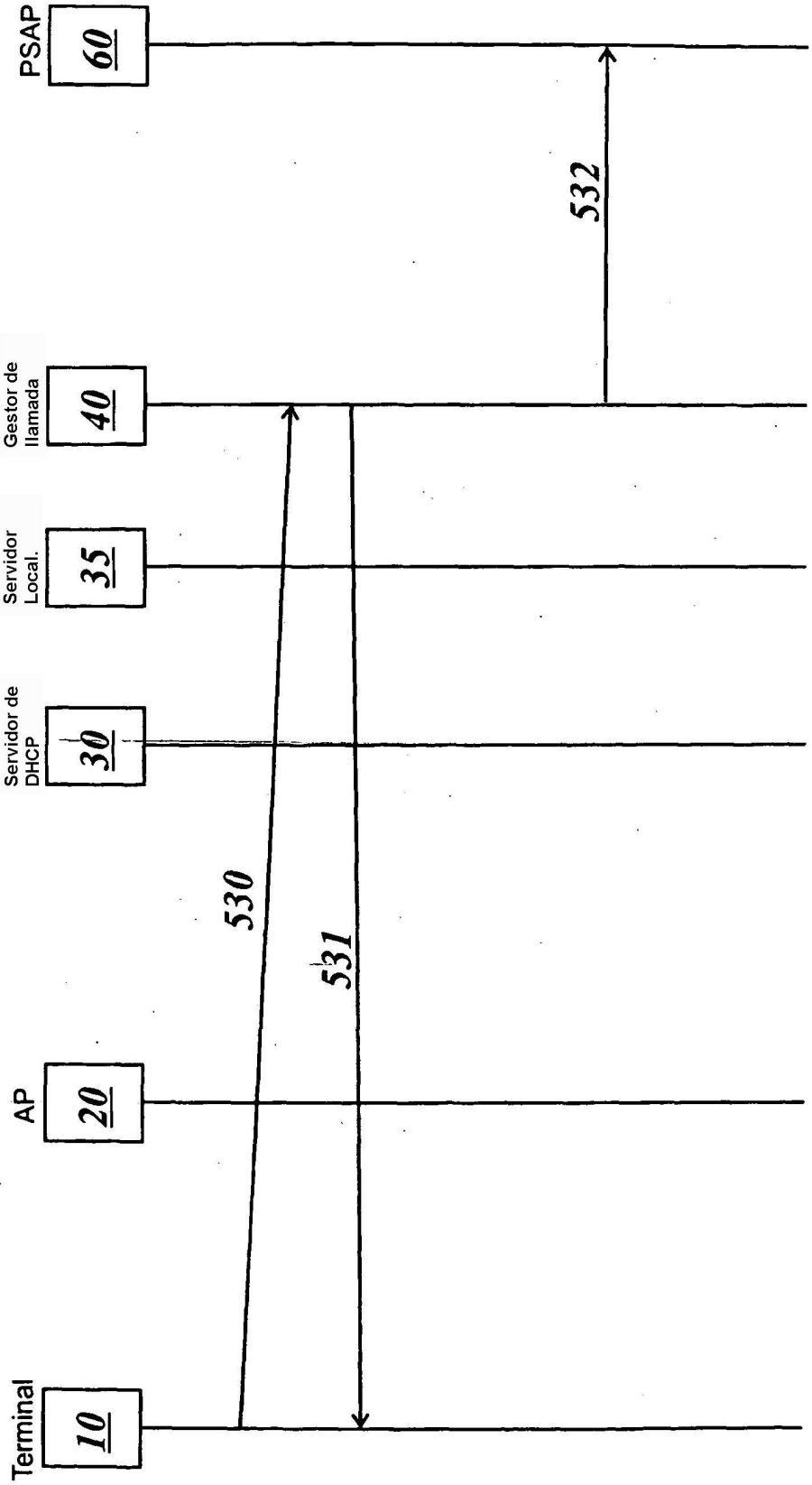
PSAP
60
532
Gestor de llamada
40
Servidor Local.
35
Servidor de DHCP
30
530
531
AP
20
Terminal
10

Fig. 6c

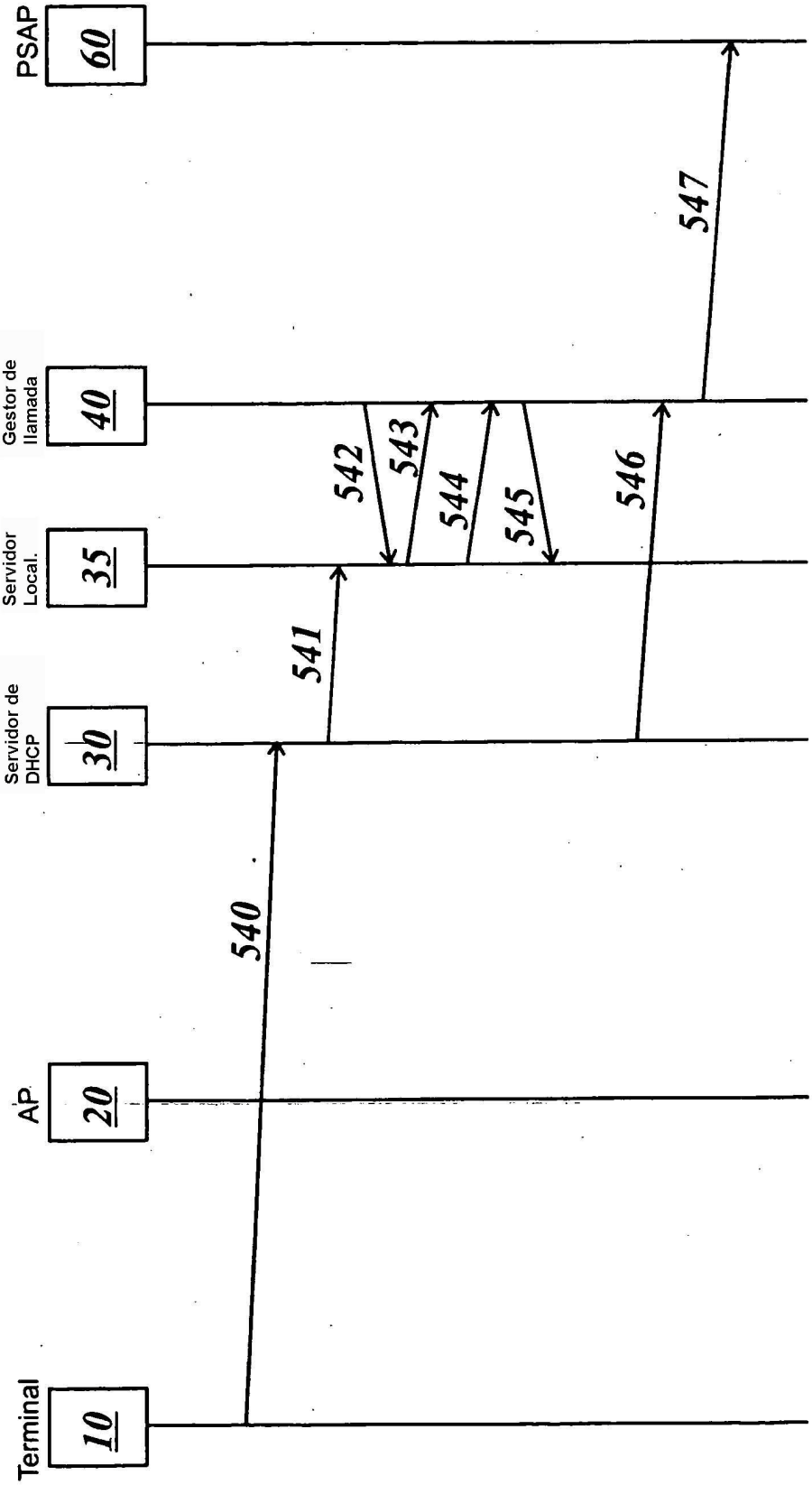
Terminal
10
AP
20
Servidor de DHCP
30
Servidor Local.
35
Gestor de llamada
40
PSAP
60
540
541
542
543
544
545
546
547

Fig. 6d