(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 361 828**

(51) Int. Cl.:
H04M 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03000281 .0**
(96) Fecha de presentación : **08.01.2003**
(97) Número de publicación de la solicitud: **1326414**
(97) Fecha de publicación de la solicitud: **09.07.2003**

(54) Título: **Transmisión segura de voz y datos a través de teléfonos IP.**

(30) Prioridad: **08.01.2002 US 346648 P**

(45) Fecha de publicación de la mención BOPI:
22.06.2011

(45) Fecha de la publicación del folleto de la patente:
22.06.2011

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

(72) Inventor/es: **Wengrovitz, Michael**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Transmisión segura de voz y datos a través de teléfonos IP.

CAMPO DE LA INVENCIÓN

Esta invención se refiere de manera general a la telefonía por Internet, y más concretamente, a proporcionar seguridad para la comunicación de telefonía por Internet.

ANTECEDENTES DE LA INVENCIÓN

En términos generales, las Redes Privadas Virtuales (VPN) son canales de comunicación seguros que proporcionan protección de datos usando técnicas de cifrado y autentificación. Las VPN se pueden implementar, por ejemplo, de acuerdo con un protocolo IPSec descrito en la Petición de Comentarios de la Fuerza de Tareas de Ingeniería de Internet 2401 titulada “Arquitectura de Seguridad para el Protocolo de Internet”, noviembre de 1998 (de aquí en adelante conocida como RFC 2401). Las VPN han llegado a ser un elemento importante en la interconexión en red de empresa para interconectar de manera segura múltiples emplazamientos corporativos, oficinas remotas, y trabajadores remotos. La tecnología VPN ayuda a asegurar que solamente pueden acceder los usuarios autorizados a los recursos de la red corporativa, y que el tráfico de datos que fluye entre dos emplazamientos no se pueda interceptar, descodificar, o burlar.

A partir de la US 2001/0043699 A1 se conocen un método y sistema para notificar al exterior que un estado de espera de un aparato de teléfono se mantiene en un momento de una respuesta a una llamada entrante. El método y sistema conocido detecta una operación de descolgado, detiene una transmisión de una llamada entrante y da instrucciones, usando una sección de función de instrucciones de generación de voz, a un generador de tonos para producir una señal de voz que informa de un estado de espera.

A partir de la GB 2 363 549 A, se conoce un método de enviar datos difundidos de forma continua sobre una red IP desde un primer nodo a un segundo nodo. El método conocido comprende usar el Intercambio de Claves de Internet (IKE) para establecer una Asociación de Seguridad (SA) IKE entre un primer y un segundo nodo. Un secreto compartido se establece entre el primer y el segundo nodo. Los datos de difusión en forma continua se cifran en el primer nodo y los datagramas IP se construyen conteniendo en sus segmentos de carga útil de los datos de difusión de forma continua cifrados. Los datagramas IP se envían entonces desde el primer nodo al segundo nodo. Los paquetes IP son paquetes VOIP.

La tecnología VPN actual permite comunicaciones de voz seguras sobre Internet a través de uno de varios métodos, que incluyen pasarelas de seguridad, ordenadores personales con las pilas IPSec, u ordenadores personales con componentes lógicos de teléfono seguro dedicados.

La FIG. 1 es un diagrama de bloques esquemático de una red que incluye los teléfonos IP convencionales 10,12 y los PC 11, 13 que transmiten y reciben los paquetes de voz sobre IP (VoIP) a través de pasarelas de seguridad 14, 16. De acuerdo con esta arquitectura, las pasarelas de seguridad 14, 16 proporcionan comunicación de voz segura sobre una red de área extensa no de confianza 18 codificando y descodificando los paquetes de VoIP. Las pasarelas de seguridad también proporcionan otros servicios de red tales como control de cortafuegos y traducción de direcciones de red (NAT). El uso de pasarelas de seguridad para IPSec algunas veces se conoce como una arquitectura puesta en el cable (BITW), o red a red VPN.

Una deficiencia con la arquitectura BITW es que se necesita comprar un dispositivo de pasarela de seguridad que tiene sus propios componentes físicos y componentes lógicos además del teléfono IP si se desea comunicación segura. Los dispositivos de pasarela de seguridad pueden ser caros. Además, tener un dispositivo de pasarela de seguridad separado implica el aumento en el consumo de potencia y la complejidad del ajuste.

La FIG. 2 es un diagrama de bloques esquemático de una red que proporciona comunicación de voz segura a través de un PC 20 sin un dispositivo de pasarela de seguridad. En su lugar, el PC 20 incluye una aplicación de componentes lógicos de telefonía IP 22 y una pila IPSec 24. La aplicación de componentes lógicos de telefonía IP proporciona la comunicación básica VoIP sobre Internet. La codificación y descodificación de los paquetes IP se hace a través de la pila IPSec 24 residente dentro del PC. De esta manera, no se necesita incurrir en costes de comprar y mantener una pasarela de seguridad separada.

El uso de la pila IPSec se puede conocer como una implementación puesta en la pila (BITS), o cliente VPN. Tal implementación, no obstante, proporciona de manera general seguridad solamente en el PC dentro del que reside la pila IPSec. La pila IPSec no se puede compartir para proporcionar comunicación de voz segura a otros aparatos y/o dispositivos de telefonía IP con los que se puede asociar.

La FIG. 3 es un diagrama de bloques esquemático de una red alternativa configurada para proporcionar comunicación de voz segura a través de un PC 30. La comunicación de voz segura se proporciona a través de componentes lógicos de teléfono seguro dedicado 32 (o componentes físicos) instalados en el PC 30. Los

componentes lógicos cifran los paquetes de VoIP usando técnicas de cifrado, tal como la basada en la técnica de Muy Buena Privacidad (PGP). Tal arquitectura se puede conocer como una implementación puesta en el código (BITC).

Un PC con componentes lógicos de teléfono seguro dedicado es susceptible de las mismas deficiencias que un PC con una pila IPSec. Es decir, los servicios de seguridad no se pueden proporcionar a aplicaciones distintas de las del PC dentro del que residen estos componentes lógicos. Además, aunque los componentes lógicos del teléfono seguro pueden proporcionar seguridad para las transmisiones de voz, no proporcionan seguridad para la transmisión de datos como se proporciona por las pasarelas de seguridad o las pilas IPSec. En su lugar, los PC con componentes lógicos de teléfono seguro transmiten datos de una manera no segura usando una pila IP 34 estándar residente en el PC. Adicionalmente, los componentes lógicos de teléfono seguro dedicados generalmente no son compatibles con IPSec y por lo tanto generalmente no son interoperables con otros dispositivos VPN.

Por consiguiente, hay una necesidad de un dispositivo de telefonía IP seguro simplificado, rentable, todo en uno para un trabajador o aplicación de oficina remota, que proporcione tanto comunicación de voz como transmisión de datos seguras, tanto para sí mismo como para dispositivos y aplicaciones IP adicionales asociadas con él.

SUMARIO DE LA INVENCIÓN

La presente invención se dirige a un aparato de teléfono IP, conocido como Teléfono Privado Virtual (VPP), en una red de comunicaciones de acuerdo con la reivindicación 1.

En una realización, el aparato de teléfono IP se configura para recibir y descodificar paquetes de datos IP además de paquetes de VoIP. El aparato de teléfono IP recibe los paquetes de datos codificados y los descodifica. Si los paquetes de datos codificados se destinan a otro dispositivo en la red de comunicaciones, el aparato de teléfono IP envía los paquetes de datos descodificados a otro dispositivo. De otro modo, invoca el primer procesador para convertir los paquetes de datos descodificados en señales de telefonía para la transmisión de voz al usuario.

En otra realización, el aparato de teléfono IP emplea distintos mecanismos de codificación en base a la dirección del dispositivo destino. En base a tal dirección destino, el segundo procesador puede decidir cifrar solamente la parte de la carga útil o tanto una cabecera como la parte de carga útil de un paquete particular.

Se debería apreciar, por lo tanto, que el aparato de teléfono IP de acuerdo con la invención proporciona comunicación de voz segura y transmisión de datos no solamente para sí mismo, sino también para otros dispositivos y aplicaciones asociadas con el aparato. De acuerdo con la invención, las aplicaciones y los dispositivos convencionales que de otro modo no serían autorizados para la comunicación segura pueden comunicar de una manera segura a través del aparato de teléfono IP. Además, el aparato de teléfono IP en sí mismo puede comunicar de manera segura sin pasarelas de seguridad adicionales u otros tipos de dispositivos de seguridad externos, permitiéndole ser más rentable y eficiente que otros dispositivos de la técnica anterior.

DESCRIPCIÓN DE LOS DIBUJOS

Estos y otros rasgos, aspectos y ventajas de la presente invención serán comprendidos más completamente cuando se consideran con respecto a la siguiente descripción detallada, las reivindicaciones adjuntas, y los dibujos anexos en los que:

La FIG. 1 es un diagrama de bloques esquemático de una red que incluye teléfonos IP y PC convencionales que transmiten y reciben los paquetes de voz sobre IP (VoIP) a través de pasarelas de seguridad;
La FIG. 2 es un diagrama de bloques esquemático de una red que proporciona comunicación de voz segura a través de un PC sin una pasarela de seguridad;
La FIG. 3 es un diagrama de bloques esquemático de una red alternativa que proporciona comunicación de voz segura a través de un PC;
La FIG. 4 es un diagrama de bloques esquemático de una red de comunicaciones que soporta telefonía IP segura y otros tipos de comunicación segura de acuerdo con una realización de la invención;
La FIG. 5 es un diagrama de bloques esquemático de un aparato de teléfono IP de acuerdo con una realización de la invención;
La FIG. 6 es un diagrama de flujo que ilustra el procesamiento de una llamada saliente iniciada por un usuario del aparato de teléfono IP de la FIG. 5 de acuerdo con una realización de la invención;
La FIG. 7A es un diagrama de flujo del procesamiento de los paquetes entrantes recibidos por el aparato de teléfono IP de la FIG. 5 sobre un interfaz LAN de acuerdo con una realización de la invención; y
La FIG. 7B es un diagrama de flujo del procesamiento de los paquetes entrantes recibidos por el aparato de teléfono IP de la FIG. 5 sobre un interfaz WAN de acuerdo con una realización de la invención; y
La FIG. 8 es un diagrama de bloques de una red de comunicaciones alternativa que soporta telefonía IP segura y otros tipos de comunicación segura de acuerdo con una realización de la invención.

DESCRIPCIÓN DETALLADA

La FIG. 4 es un diagrama de bloques de una red de comunicaciones que soporta telefonía IP segura y otros tipos de comunicación segura de acuerdo con una realización de la invención. En la realización ilustrada, la red incluye un aparato de teléfono IP 40 acoplado a una red de área extensa (WAN) 50 y una red de área local (LAN) 48 sobre cables y/u otros medios de transmisión tales como un medio inalámbrico. La WAN 50 puede ser una WAN privada o una WAN pública tal como una Internet pública.

El aparato de teléfono IP 40 comunica con los teléfonos IP 42, los PC 44, y otros dispositivos de red 46 en la LAN usando un medio de comunicación LAN, tal como Ethernet o Token Ring. Los medios de comunicación LAN Ethernet no se limitan a 10 megabit Ethernet, sino que incluyen otras variantes, tales como Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet y Ethernet inalámbrica 802.11b. El aparato de teléfono IP 40 también comunica con un ordenador central 54 en un emplazamiento central 52 sobre la WAN 50 usando un protocolo de comunicación tal como, por ejemplo, un protocolo TCP/IP.

De acuerdo con una realización, el aparato de teléfono IP 40 es un teléfono IP que incorpora el aspecto y sensación de un teléfono tradicional con un teclado, botones de función, auricular, y pantalla. A diferencia de un teléfono tradicional, no obstante, el aparato de teléfono IP está mejorado con la capacidad de proporcionar telefonía IP y comunicación de datos seguras sobre la WAN para sí mismo así como para uno o más de los dispositivos de red 42, 44, 46 en la LAN 48. Esta arquitectura se puede conocer como una arquitectura puesta en el teléfono (BITP).

En las realizaciones alternativas, el aparato de teléfono IP 40 se puede implementar como un teléfono portátil, asistente digital portátil (PDA), ordenador personal, o cualquier otro dispositivo de usuario final cableado o inalámbrico que es convencional en la técnica.

Un usuario puede usar el aparato de teléfono IP 40 para iniciar y recibir llamadas de teléfono seguras con el ordenador central 54 en el emplazamiento central 52 sobre la WAN 50 usando cualquier interfaz WAN que es convencional en la técnica. El emplazamiento central 52 puede incluir un dispositivo para proporcionar la comunicación segura para el ordenador central 54, tal como, por ejemplo, una pasarela de seguridad 55 acoplada al ordenador central.

Además, el aparato de teléfono IP 40 recibe los paquetes de voz y datos desde los dispositivos 42, 44, 46 en la LAN 48, asegura los paquetes, y transmite los paquetes asegurados o bien al ordenador central 54 o bien a otro dispositivo de destino remoto. El aparato de teléfono IP 40 también recibe los paquetes de voz y datos entrantes asegurados, descodifica estos paquetes, y o bien los proporciona al usuario del aparato o bien los envía a uno de los dispositivos de destino en la LAN.

Además de lo anterior, el aparato de teléfono IP 40 incluye capacidad NAT y cortafuegos para prevenir el acceso no autorizado. En este sentido, el aparato de teléfono IP 40 asegura la voz en sí misma y en nombre de sus clientes, y también proporciona protección de cortafuegos para su teléfono y en nombre de sus clientes LAN.

La FIG. 5 es un diagrama de bloques esquemático más detallado del aparato de teléfono IP 40 de acuerdo con una realización de la invención. En la realización ilustrada, el aparato 40 incluye un aparato de teléfono digital 60 acoplado a un procesador digital de señal (DSP) 62 y procesador central 64. El procesador central además se acopla a dos interfaces de red 70, 72. De acuerdo con una realización, el primer interfaz de red 70 se usa para comunicar con los dispositivos 42, 44, 46 en la LAN 48 y el segundo interfaz de red 72 se usa para comunicar con el ordenador central 54 sobre la WAN 50.

El procesador central 64 incluye una pila de seguridad 68 y una pila de protocolo de red 66. Las pilas de protocolo de seguridad y red 68, 66 se pueden implementar en los componentes lógicos, componentes físicos, microprogramas (por ejemplo a través de un circuito integrado de aplicaciones específicas), o en cualquier combinación de los mismos. Por ejemplo, las pilas de protocolo de seguridad y red pueden ser procesadores separados que implementan los algoritmos de seguridad y la VoIP. Alternativamente, las pilas de protocolo de seguridad y red pueden ser rutinas de programas informáticos ejecutados en un único procesador.

De acuerdo con una realización de la invención, la pila de seguridad 68 es una pila IPSec según se establece en adelante en la RFC 2401. La pila de protocolo de red puede ser una pila de protocolo de transporte convencional tal como, por ejemplo, una pila H.323, pila de Protocolo de Inicio de Sesión (SIP), pila de protocolo de control de pasarela de medios (MGCP), o similares. Una persona experta en la técnica debería reconocer que otros tipos de protocolos de transporte y mecanismos de seguridad convencionales pueden ser utilizados como se conoce en la técnica sin estar limitados a los protocolos y los mecanismos de seguridad revelados.

La FIG. 6 es un diagrama de flujo que ilustra el procesamiento de una llamada saliente iniciada por un usuario del aparato de teléfono IP 40 de acuerdo con una realización de la invención. El proceso empieza cuando un usuario del aparato de teléfono IP 40 utiliza el aparato de teléfono digital 60 para iniciar la llamada saliente de acuerdo con los

mecanismos convencionales. En el paso 80, el procesador central 64 recibe una petición para iniciar la llamada desde el aparato digital, y en el paso 81, intenta establecer una asociación de seguridad (SA) con el dispositivo destinatario de la llamada como se fija en adelante en la RFC 2401.

Las señales de voz iniciadas por el usuario se proporcionan al aparato de teléfono digital 60 que digitaliza y envía las señales al DSP 62 en el paso 82. En el paso 83, el DSP 62 segmenta, comprime, y empaqueta las señales de voz de una manera que es convencional en la técnica. Si la negociación de la SA del paso 81 no tuvo éxito, como se determina en el paso 84, el procesador central 64 transmite los paquetes de voz al dispositivo destinatario de la llamada a través de su interfaz de red WAN 72 sin cifrar los paquetes. Alternativamente, con un ajuste distinto de la gestión/configuración del teléfono IP, el procesador central 64 no transmite el paquete de voz de ninguna manera.

De otro modo, si la negociación de la SA tuvo éxito, el procesador central 64 invoca a la pila de seguridad 68 para codificar los paquetes de voz en el paso 86 de una manera bien conocida en la técnica. De acuerdo con una realización, la pila de seguridad codifica los paquetes de voz de la misma manera sin tener en cuenta el destino de los paquetes. De acuerdo con otra realización, la pila de seguridad emplea distintos mecanismos de codificación dependiendo de la fuente, destino, puerto, u otros selectores como se identifica en la RFC 2401. Por ejemplo, se puede utilizar un modo de transporte de cifrado para codificar los paquetes de voz transmitidos a un dispositivo en la LAN 48, que provoca que solamente sean codificados los datos de la la carga útil, mientras que se puede utilizar un modo túnel de cifrado para codificar los paquetes de voz transmitidos a otro dispositivo fuera de la LAN, provocando tanto que sea codificada tanto la cabecera como los datos de la carga útil.

Una vez que los paquetes de voz se codifican, el procesador 64 invoca, en el paso 87, la pila del protocolo de red 66 para transmitir los paquetes de voz codificados a sus destinos en la LAN 48 o sobre la WAN 50 a través de los interfaces de red respectivos 72, 70.

La FIG. 7A es un diagrama de flujo del procesamiento de los paquetes de voz o datos entrantes recibidos por el aparato de teléfono IP 40 sobre su interfaz LAN de acuerdo con una realización de la invención. En el paso 90, el aparato de teléfono IP 40 recibe un paquete entrante comunicado por uno de los dispositivos de red 42, 44, 46 en la LAN 48, a través del primer interfaz de red 70. El paquete se envía al procesador central 64 el cual, en el paso 92, examina los datos de la cabecera del paquete para determinar si el aparato de teléfono IP 92 es el destino definitivo. Si la respuesta es NO, el procesador central 64 determina si la pila de seguridad 68 va a ser invocada para codificar el paquete anterior a enviar a su destino. Si la respuesta es NO, el procesador central 64 determina si la pila de seguridad 68 va a ser invocada para codificar el paquete previo a enviar a su destino.

Varios factores pueden determinar si codificar el paquete, y en caso afirmativo, el tipo de codificación a ser realizada. Por ejemplo, si el paquete recibido ya ha sido codificado por el dispositivo de transmisión por sí mismo, no se puede realizar la codificación. Alternativamente, el aparato de teléfono IP puede decidir codificar el paquete incluso si ya se codificó, pero usando un modo distinto de cifrado que el empleado por el dispositivo de codificación.

En otro ejemplo, el aparato de teléfono IP 40 no puede codificar el paquete si va a ser enviado a otro dispositivo en la LAN 48, o si la codificación va a ser hecha, solamente se puede codificar los datos de la carga útil a través del mecanismo de cifrado de transporte. No obstante, si el paquete se va a enviar a un dispositivo fuera de la LAN, tanto la cabecera como los datos de la carga útil se pueden codificar a través del mecanismo de cifrado de túnel.

Aún en otro ejemplo, la determinación de la codificación se puede basar en si fue negociada con éxito una SA con el destino definitivo. El paquete se codifica si se hizo con éxito una negociación SA.

Si la pila de seguridad 68 determina que el paquete se debería codificar, el paquete se codifica en el paso 96, y el paquete codificado se transmite a su destino en el paso 98. De otro modo, si no se va a hacer ninguna codificación, el paquete se transmite al destino sin codificar.

Con referencia de nuevo al paso 92, si el aparato de teléfono IP 40 es el destino definitivo, se hace una determinación en cuanto a si el paquete recibido es un paquete codificado que necesita ser descodificado, como se determina en el paso 100. En el paso 102, la pila de seguridad 68 pasa a descodificar el paquete, y transmite el paquete descodificado al DSP 62.

Si el paquete es un paquete de VoIP, el DSP 62, en el paso 104, convierte el paquete a una señal de voz. En el paso 106, los datos o la señal convertida se transmiten al aparato de teléfono 60.

La FIG. 7B es un diagrama de flujo del procesamiento de los paquetes de voz o datos entrantes recibidos por el aparato de teléfono IP 40 sobre un interfaz WAN de acuerdo con una realización de la invención. En el paso 110, el aparato de teléfono IP 40 recibe un paquete de voz o datos entrante comunicado por el ordenador central 54 sobre la WAN 50 a través del segundo interfaz 72. El paquete se envía al procesador central 64 el cual, en el paso 111, determina de acuerdo con los mecanismos convencionales si el paquete ha sido codificado. Si el paquete ha sido codificado, la pila de seguridad 68 pasa a descodificar el paquete en el paso 112.

En el paso 113, el procesador central 64 examina los datos de la cabecera del paquete descodificado para determinar si el aparato de teléfono IP 92 es el destino definitivo. Si la respuesta es NO, el paquete descodificado se envía a su destino definitivo en el paso 114.

De otro modo, si el destino definitivo del paquete es el dispositivo de teléfono IP 40, el paquete se transmite al DSP 62. Si el paquete es un paquete de VoIP, el DSP 62, en el paso 115, convierte el paquete a una señal de voz. En el paso 116, la señal convertida se transmite al aparato de teléfono 60.

La FIG. 8 es un diagrama de bloques de una red de comunicaciones alternativa que soporta telefonía IP segura y otros tipos de comunicación segura de acuerdo a una realización de la invención. La red incluye los aparatos de teléfono IP 120, 122, acoplados a una LAN 140 sobre un primer interfaz de red 132, 134, y a un ordenador central 126, 128 sobre un segundo interfaz de red 136, 138. La LAN 140 se acopla a su vez a una pasarela 124 que proporciona el acceso a una WAN 130 de una manera que es convencional en la técnica. La LAN 140 también puede soportar otros dispositivos tales como un PC 142, un PC con una pila IPSec interna 144, una PBX IP 146, y un servidor corporativo 148.

Los aparatos de teléfono IP 120, 122 son similares al aparato de teléfono IP 40 de las FIG. 4 y 5. Una diferencia, no obstante, es el uso de uno de los interfaces de red para conectar al ordenador central 126, 128.

Los ordenadores centrales 126, 128 pueden ser dispositivos de usuario final cableados o inalámbricos tales como PC, teléfonos IP convencionales, PDA, o similares. Aunque la FIG. 8 representa solamente un ordenador central agregado a cada aparato de teléfono IP 120, 122 una persona experta en la técnica debería reconocer que se podrían agregar múltiples ordenadores centrales.

La pasarela 124 puede ser una pasarela convencional que proporciona el acceso a la WAN 130, y puede proporcionar otros tipos de servicios de red tales como NAT, y cortafuegos, y/o servicios IPSec. En la realización en la que la pasarela 124 proporciona los servicios IPSec, la pasarela se puede implementar como una pasarela de seguridad similar a la pasarela de seguridad 14, 16 de la FIG. 1.

De acuerdo con la realización ilustrada en la FIG. 8, un ordenador central 126 o 128 transmite un paquete, tal como un paquete de mensaje instantáneo, a su aparato de teléfono IP respectivo 120, 122. El aparato de teléfono IP intenta establecer una SA IPSec con un dispositivo de destino. Si la negociación de la SA entre un ordenador central y el destino no tiene éxito, el paquete se transmite al destino de una manera desprotegida sin codificar. En una realización alternativa, el paquete no se transmite de ningún modo.

No obstante, si el dispositivo de destino tiene una pila IPSec interna, tal como es el caso con el PC 144, o se agrega a uno de los aparatos de teléfono IP 120, 122, tal como el ordenador central 126 o 128, la negociación de la SA es exitosa. El paquete se codifica entonces por el aparato de teléfono IP y se transmite al destino de una manera segura.

De acuerdo con una realización, el aparato de teléfono IP 120, 122 determina el tipo de codificación en base a la información de destino. De acuerdo con una realización, una tabla de direcciones IP (no se muestra) indica si una conexión a la dirección indicada va a estar basada en un modo de transporte de cifrado o un modo túnel de cifrado. Si se indica el modo de transporte de cifrado, solamente se cifra una parte de la carga útil del paquete como se proporciona por IPSec. Si se indica el modo túnel de cifrado, se cifran tanto una dirección como la parte de la carga útil del paquete como también se proporciona por IPSec. La dirección de la pasarela de seguridad también se puede cifrar en el modo túnel de cifrado. Los paquetes de VoIP no se pueden codificar de la manera descrita anteriormente.

Por ejemplo, la tabla de direcciones IP puede indicar el modo transporte de cifrado para las direcciones de los dispositivos de destino que residen en la LAN 140. No obstante, si el destino reside en la LAN 140 detrás de la pasarela 124, o en la WAN 130, una red inherentemente no digna de confianza, la tabla de direcciones IP puede indicar el modo túnel de cifrado.

De acuerdo con otra realización, si la pasarela 124 es una pasarela de seguridad que implementa el modo túnel de cifrado, el aparato de teléfono IP 120, 122 cifra los paquetes de acuerdo con el modo de transporte de cifrado para todos los paquetes sin tener en cuenta su destino. De esta manera, los paquetes a ser transmitidos sobre la LAN se cifran solamente en el área de la carga útil por el aparato de teléfono IP 120, 122 mientras que los paquetes a ser transmitidos a los dispositivos detrás de la pasarela 124, tales como, por ejemplo, a los dispositivos en la WAN 130, se cifran en el área de la carga útil por el aparato de teléfono IP 120, 122 y en ambos las áreas de la carga útil y cabecera por la pasarela de seguridad 124, que proporciona doble seguridad para el paquete.

Aunque esta invención se ha descrito en ciertas realizaciones específicas, aquellos expertos en la técnica no tendrán dificultad en la elaboración de variaciones las cuales de ninguna manera se separen del alcance de la presente invención. Por lo tanto se va a entender que esta invención se puede practicar de otro modo del que se

describe específicamente. De esta manera, las presentes realizaciones de la invención se deberían considerar en todas las consideraciones como ilustrativas y no restrictivas, el alcance de la invención que se indica por las reivindicaciones adjuntas y sus equivalente más que la descripción anteriormente mencionada.

REIVINDICACIONES

1. Un aparato de teléfono del protocolo de Internet, IP, (40) en una red de comunicaciones que comprende:

una entrada de voz;
una salida de voz; y
al menos un módulo de procesamiento (64);
caracterizado porque:

la entrada de voz recibe señales de voz entrantes desde un usuario;
el al menos un módulo de procesamiento (64) convierte las señales de voz entrantes en paquetes de voz IP salientes, codifica los paquetes de voz IP salientes y transmite los paquetes de voz IP salientes a un dispositivo de destino;
el al menos un módulo de procesamiento (64) recibe los paquetes de voz IP entrantes codificados por un dispositivo fuente, descodifica los paquetes de voz IP entrantes, y si los paquetes descodificados se destinan a otro dispositivo en la red de comunicaciones, envía los paquetes descodificados al otro dispositivo, y de otro modo convierte los paquetes descodificados en señales de voz salientes y transmite las señales de voz salientes al usuario a través de la salida de voz; y
el al menos un módulo de procesamiento (64) codifica y descodifica los paquetes de acuerdo con un protocolo de seguridad IP (68).

2. El aparato de teléfono IP (40) de la reivindicación 1 que además comprende:

un interfaz de red de área extensa para la transmisión de los paquetes de voz IP salientes codificados por el al menos un módulo de procesamiento (64) y para recibir los paquetes de voz IP entrantes codificados por el dispositivo fuente; y
un interfaz de red de área local para enviar los paquetes de voz IP entrantes descodificados por el al menos un módulo de procesamiento (64).

3. El aparato de teléfono IP (40) de la reivindicación 1 que además comprende un interfaz de red de área local para recibir los paquetes de voz IP o datos desde el segundo dispositivo fuente y un interfaz de red de área extensa para transmitir los paquetes codificados al segundo dispositivo destino.

4. El aparato de teléfono IP (40) de la reivindicación 1 que además comprende un interfaz de red de área local para recibir los paquetes de voz IP o datos desde el segundo dispositivo fuente y para transmitir los paquetes codificados al segundo dispositivo destino.

5. El aparato de teléfono IP (40) de la reivindicación 1 caracterizado además porque el al menos un módulo de procesamiento (64), en la codificación de un paquete particular, determina si cifrar una parte de la carga útil del paquete particular o tanto la cabecera como la parte de la carga útil del paquete particular en base a una dirección del dispositivo destino.

6. El aparato de teléfono IP (40) de la reivindicación 1, en el que un primer módulo de procesamiento (64) convierte las señales de voz entrantes en los paquetes de voz IP salientes, y además convierte los paquetes descodificados en las señales de voz salientes y transmite las señales de voz salientes al usuario a través de la salida de voz, y en el que un segundo módulo de procesamiento (64) codifica los paquetes de voz IP salientes y transmite los paquetes de voz IP salientes al dispositivo destino, y además recibe los paquetes de voz IP entrantes codificados por el dispositivo fuente, descodifica los paquetes de voz IP entrantes , y si los paquetes descodificados se destinan para el otro dispositivo en la red de comunicaciones, envía los paquetes descodificados al otro dispositivo, e invoca de otro modo el primer módulo de procesamiento (64) para convertir los paquetes descodificados en las señales de voz salientes y transmitir las señales de voz salientes al usuario a través de la salida de voz.

7. El aparato de teléfono IP (40) de la reivindicación 1, en el que al menos un módulo de procesamiento (64) proporciona la protección cortafuegos para prevenir el acceso no autorizado.

8. Un método para proporcionar comunicación a través de un aparato de teléfono de protocolo de Internet, IP, (40) que tiene una entrada de voz, salida de voz, y al menos un módulo de procesamiento (64), estando el método **caracterizado por**:

recibir señales de voz entrantes desde un usuario a través de la entrada de voz;
usar el al menos un módulo de procesamiento (64) para convertir las señales de voz entrantes en paquetes de voz IP salientes;
usar el al menos un módulo de procesamiento (64) para codificar los paquetes de voz IP salientes;
transmitir los paquetes de voz IP salientes a un dispositivo de destino;

recibir los paquetes de voz IP entrantes codificados por un dispositivo fuente;
usar el al menos un módulo de procesamiento (64) para descodificar los paquetes de voz IP entrantes;
si los paquetes descodificados se destinan a otro dispositivo en la red de comunicaciones, enviar los paquetes descodificados al otro dispositivo; y
si los paquetes descodificados se destinan al aparato de teléfono IP (40):

usar el al menos un módulo de procesamiento (64) para convertir los paquetes descodificados en señales de voz salientes; y
transmitir las señales de voz salientes a la salida de voz; y

usar el al menos un módulo de procesamiento (64) para codificar y descodificar los paquetes de acuerdo con un protocolo de seguridad IP (68).

9. El método de la reivindicación 8, en el que se usa un interfaz de red de área extensa para transmitir los paquetes de voz IP salientes codificados por el al menos un módulo de procesamiento (64) y para recibir los paquetes de voz IP entrantes codificados por el dispositivo fuente, y se usa un interfaz de red de área local para enviar los paquetes de voz IP entrantes descodificados por el al menos un módulo de procesamiento (64).

10. El método de la reivindicación 9, en el que se usa un interfaz de red de área local para recibir los paquetes de voz IP o datos desde el segundo dispositivo fuente y se usa un interfaz de red de área extensa para transmitir los paquetes codificados al segundo dispositivo de destino.

11. El método de la reivindicación 9, en el que se usa un interfaz de red de área local para recibir los paquetes de voz IP o datos desde el segundo dispositivo fuente y para transmitir los paquetes codificados al segundo dispositivo de destino.

12. El método de la reivindicación 9, en el que la codificación además comprende:

determinar en base a una dirección del dispositivo de destino si cifrar una parte de la carga útil de los paquetes de voz o datos o tanto una cabecera como la parte de la carga útil de los paquetes de voz o datos.

13. El método de la reivindicación 9, en el que la codificación además comprende:

determinar en base a una dirección del dispositivo de destino si cifrar una parte de la carga útil de los paquetes de voz IP o tanto una cabecera como la parte de la carga útil de los paquetes de voz IP salientes.

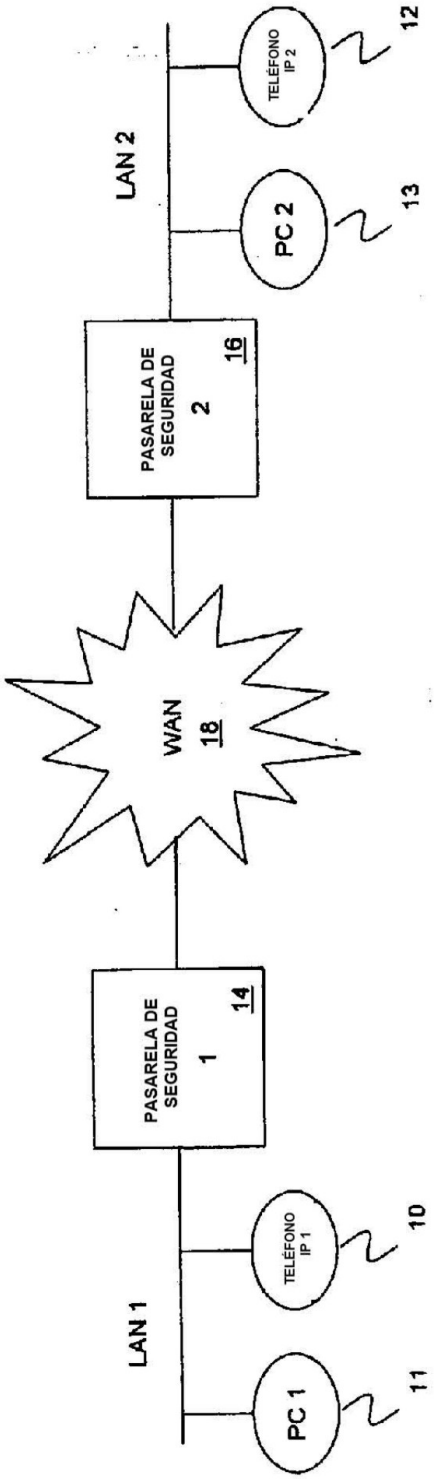

FIG. 1
(TÉCNICA ANTERIOR)

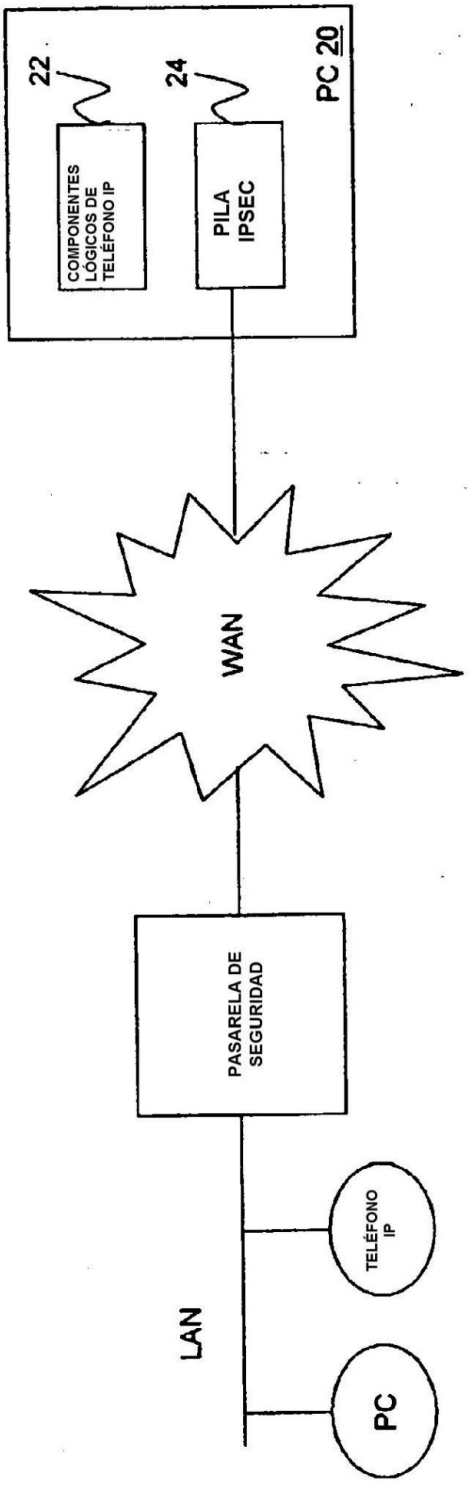

FIG. 2
(TÉCNICA ANTERIOR)

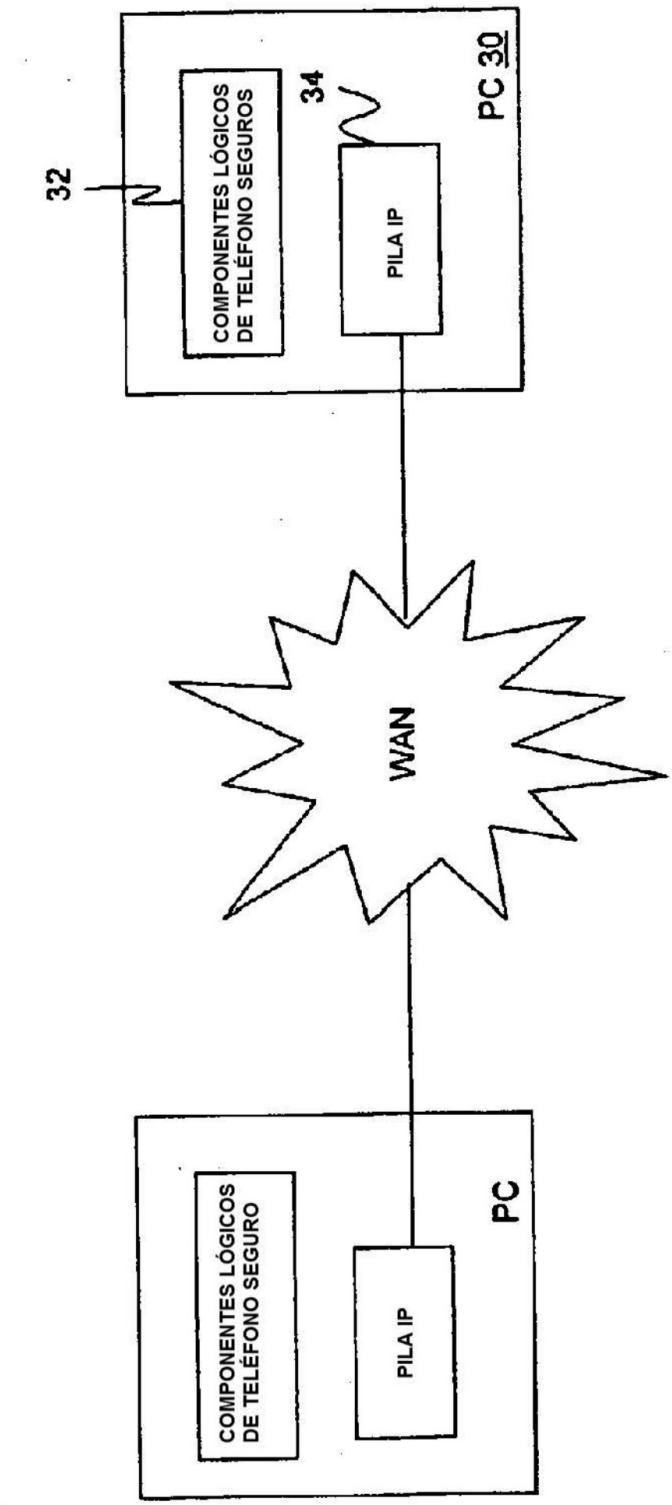

FIG. 3
(TÉCNICA ANTERIOR)

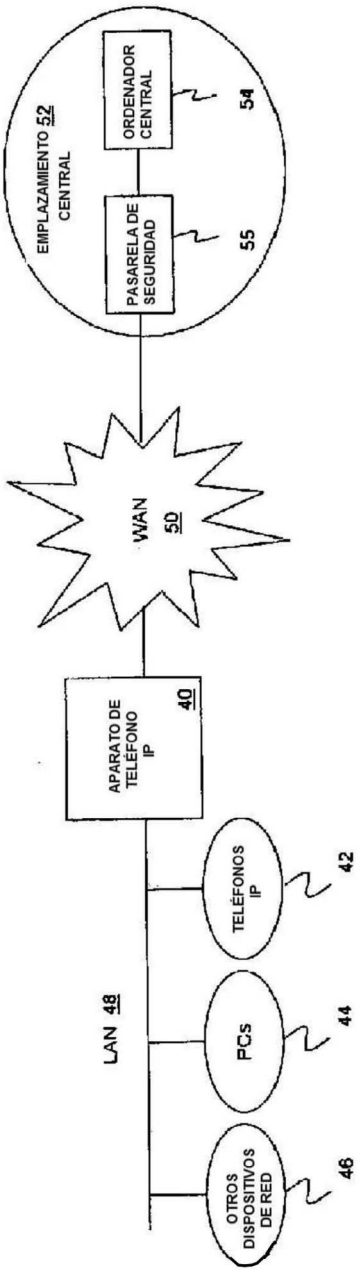
EMPLAZAMIENTO 52
CENTRAL
ORDENADOR CENTRAL
54
PASARELA DE SEGURIDAD
55
WAN
50
APARATO DE TELÉFONO IP
40
LAN 48
TELÉFONOS IP
42
PCs
44
OTROS DISPOSITIVOS DE RED
46

FIG. 4

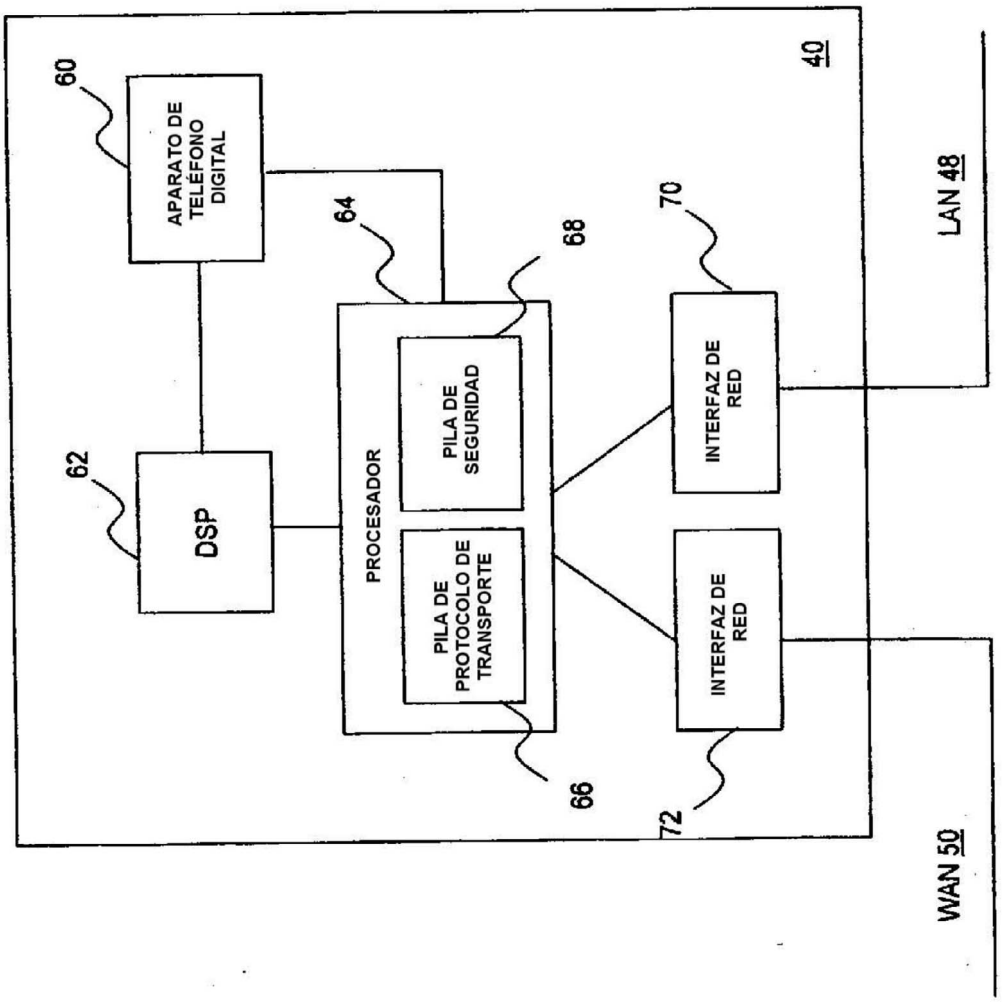
40
60
APARATO DE TELÉFONO DIGITAL
62
DSP
64
PROCESADOR
68
PILA DE SEGURIDAD
66
PILA DE PROTOCOLO DE TRANSPORTE
70
INTERFAZ DE RED
72
INTERFAZ DE RED
LAN 48
WAN 50

FIG. 5

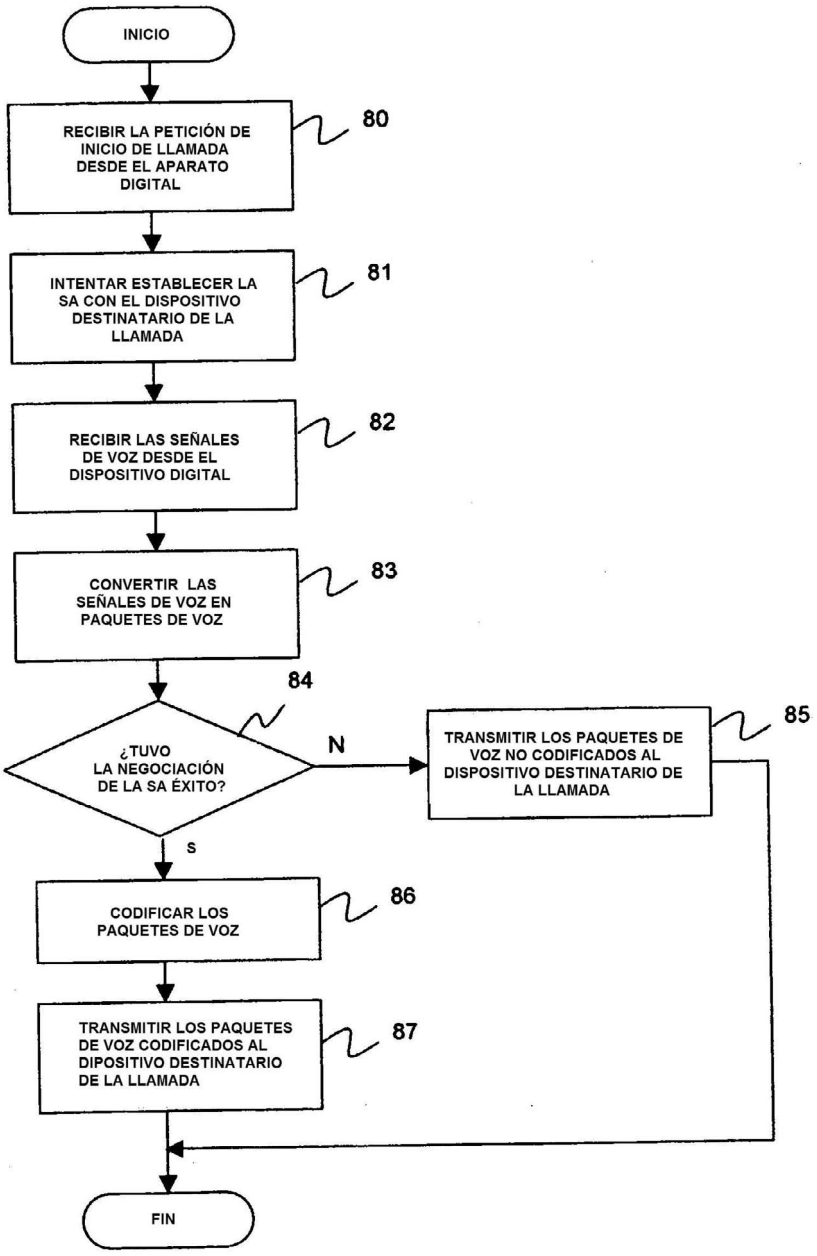
INICIO
RECIBIR LA PETICIÓN DE INICIO DE LLAMADA DESDE EL APARATO DIGITAL
80
INTENTAR ESTABLECER LA SA CON EL DISPOSITIVO DESTINATARIO DE LA LLAMADA
81
RECIBIR LAS SEÑALES DE VOZ DESDE EL DISPOSITIVO DIGITAL
82
CONVERTIR LAS SEÑALES DE VOZ EN PAQUETES DE VOZ
83
84
¿TUVO LA NEGOCIACIÓN DE LA SA ÉXITO?
N
TRANSMITIR LOS PAQUETES DE VOZ NO CODIFICADOS AL DISPOSITIVO DESTINATARIO DE LA LLAMADA
85
S
CODIFICAR LOS PAQUETES DE VOZ
86
TRANSMITIR LOS PAQUETES DE VOZ CODIFICADOS AL DIPOSITIVO DESTINATARIO DE LA LLAMADA
87
FIN

FIG. 6

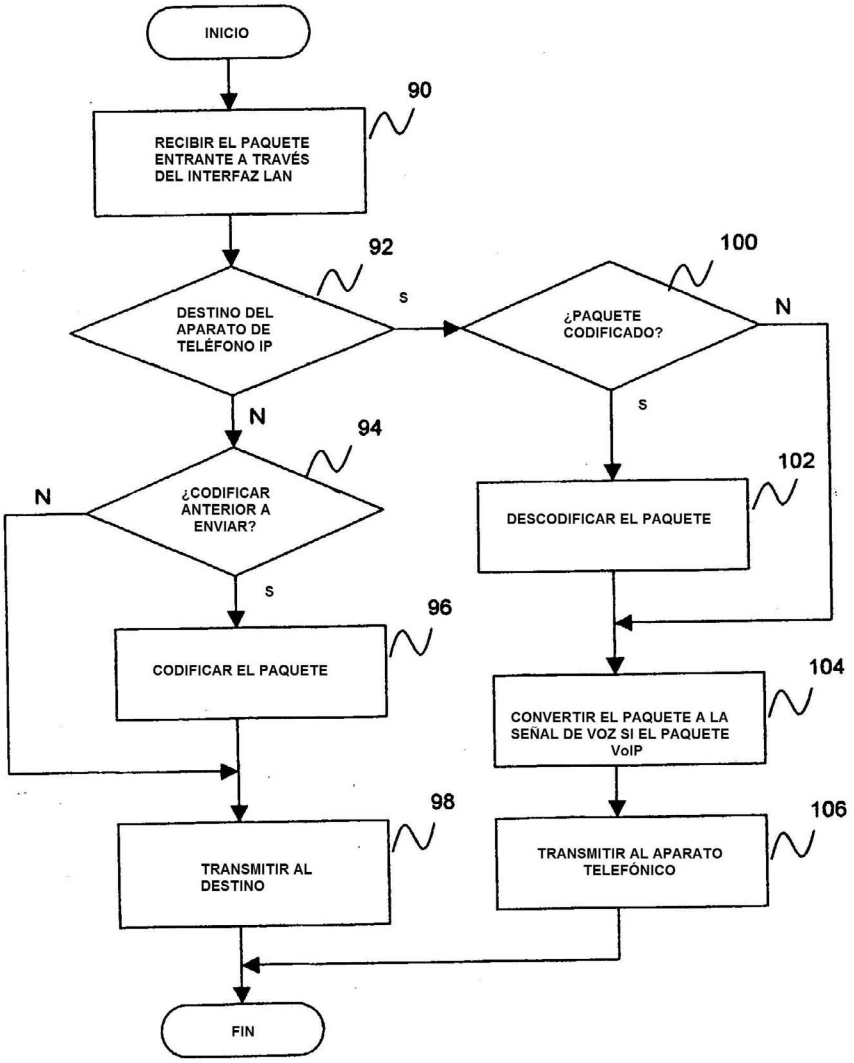
INICIO
90
RECIBIR EL PAQUETE ENTRANTE A TRAVÉS DEL INTERFAZ LAN
92
DESTINO DEL APARATO DE TELÉFONO IP
S
100
¿PAQUETE CODIFICADO?
N
S
N
94
¿CODIFICAR ANTERIOR A ENVIAR?
N
S
102
DESCODIFICAR EL PAQUETE
96
CODIFICAR EL PAQUETE
104
CONVERTIR EL PAQUETE A LA SEÑAL DE VOZ SI EL PAQUETE VoIP
98
TRANSMITIR AL DESTINO
106
TRANSMITIR AL APARATO TELEFÓNICO
FIN

FIG. 7A

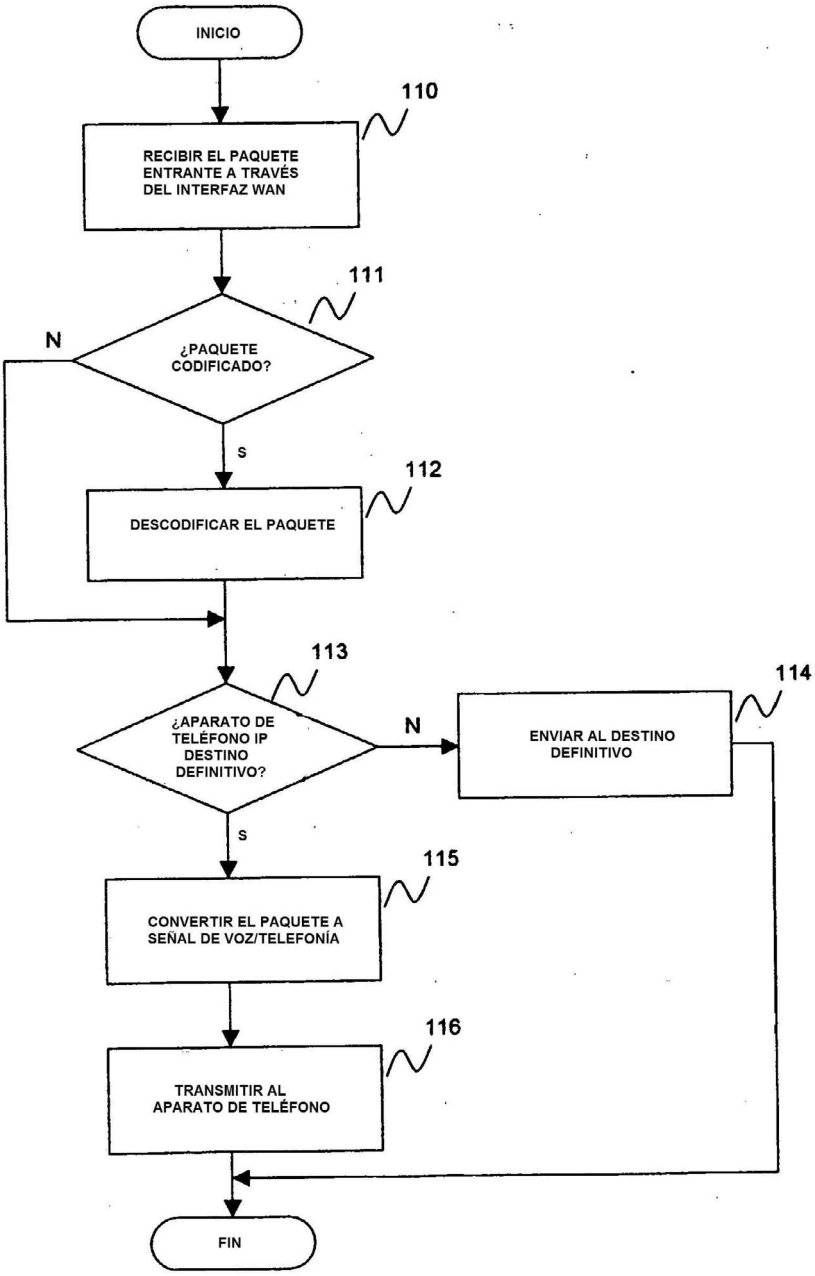
INICIO
110
RECIBIR EL PAQUETE ENTRANTE A TRAVÉS DEL INTERFAZ WAN
111
¿PAQUETE CODIFICADO?
N
S
112
DESCODIFICAR EL PAQUETE
113
¿APARATO DE TELÉFONO IP DESTINO DEFINITIVO?
N
114
ENVIAR AL DESTINO DEFINITIVO
S
115
CONVERTIR EL PAQUETE A SEÑAL DE VOZ/TELEFONÍA
116
TRANSMITIR AL APARATO DE TELÉFONO
FIN

FIG. 7B

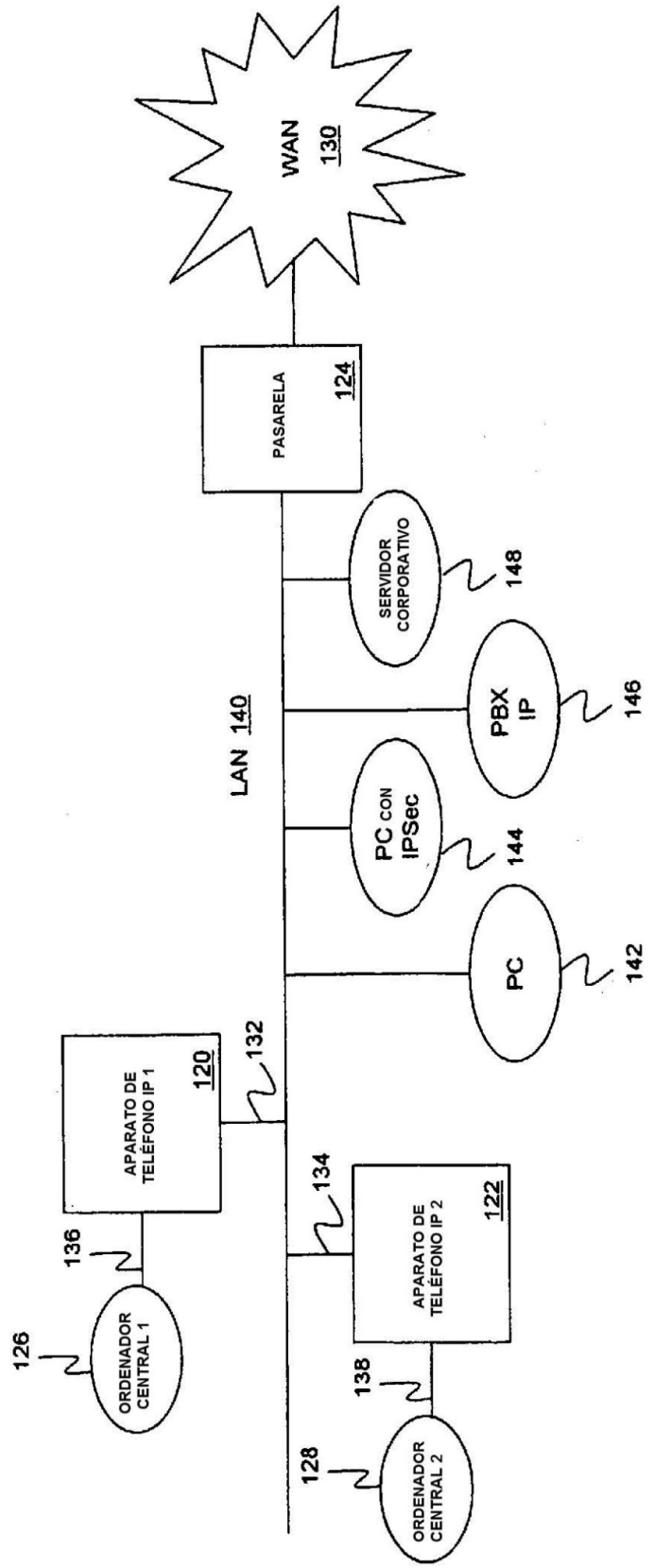
WAN
130
PASARELA
124
SERVIDOR CORPORATIVO
148
PBX IP
146
PC CON IPSec
144
PC
142
LAN 140
APARATO DE TELÉFONO IP 1
120
132
APARATO DE TELÉFONO IP 2
122
134
ORDENADOR CENTRAL 1
136
126
ORDENADOR CENTRAL 2
138
128

FIG. 8