(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 704 473**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/66 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.02.2010 PCT/CA2010/000167**

(87) Fecha y número de publicación internacional: **12.08.2010 WO10088774**

(96) Fecha de presentación y número de la solicitud europea: **05.02.2010 E 10738189 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.10.2018 EP 2394414**

(54) Título: **Atravesamiento de NAT usando perforación de agujero**

(30) Prioridad:

06.02.2009 US 150378 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2019

(73) Titular/es:

XMEDIUS SOLUTIONS INC. (100.0%)
1135-3400 Boul. De Maisonneuve O.
Montreal, QC H3Z 3B8, CA

(72) Inventor/es:

BOIRE-LAVIGNE, SEBASTIEN;
COLETTE, RICHARD;
LALONDE, SEBASTIEN y
MALENFANT, ERIC

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Atravesamiento de NAT usando perforación de agujero

Solicitud relacionada

Esta solicitud reivindica el beneficio de la Solicitud de Patente Provisional de Estados Unidos 61/150378, presentada el 6 de febrero de 2009.

Antecedentes

La presente invención se refiere en general al atravesamiento de un traductor de dirección de red y, más particularmente, a una solución escalable para atravesar un traductor de dirección de red simétrico para VoIP (VoIP) y otras sesiones de comunicación.

La Internet es un sistema global de muchas redes informáticas interconectadas, tanto públicas como privadas. La Internet permite la conectividad de extremo a extremo directa entre dos dispositivos o puntos finales usando protocolos convencionales tales como el Protocolo de Internet (IP), el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagrama de Usuario (UDP). Cada dispositivo conectado a la Internet tiene asignado una dirección de IP que posibilita el encaminamiento de paquetes de datos. Actualmente, la mayoría de los dispositivos usan el esquema de dirección especificado en el Protocolo de Internet Versión 4 (IPv4). La arquitectura abierta y la accesibilidad casi universal de la Internet han conducido a una adopción y uso extendidos de la Internet por las empresas y los individuos.

Las características que hacen a la Internet tan conocida también contribuyen a algunas de sus desventajas. Por ejemplo, la conectividad de acceso universal y de extremo a extremo directa posibilita que usuarios en lados opuestos del globo comuniquen directamente entre sí, pero expone los ordenadores a hackers y a otras terceras partes maliciosas. La conectividad de extremo a extremo directa también requiere que a cada dispositivo se le proporcione una única dirección de IP. Sin embargo, la adopción extendida de la Internet ha conducido la reducción de direcciones disponibles en el espacio de direcciones de IPV4.

Para tratar problemas de seguridad, la mayoría de las redes empresariales y domésticas privadas implementan ahora alguna forma de cortafuegos. Un cortafuegos comprende hardware y/o software que están diseñados para bloquear acceso no autorizado a una red protegida mientras permiten comunicaciones autorizadas con usuarios fuera del cortafuegos. Los cortafuegos protegen contra acceso no autorizado aplicando una política de seguridad predefinida a paquetes que entran en una red protegida. La política de seguridad comprende un conjunto de reglas y procedimientos que rigen paquetes de datos que entran o salen de la red protegida. El cortafuegos permite que los paquetes pasen a través del cortafuegos basándose en las reglas específicas de la política definida. Más a menudo, un cortafuegos permite que la mayoría de los paquetes salientes que se originan desde el interior de la red protegida pasen a través del cortafuegos mientras que bloquea la mayoría de los paquetes entrantes de la red pública. El tráfico de datos de las redes públicas se permite que pase únicamente si se ajusta a un filtro de control de acceso definido, se envía en respuesta a un paquete de datos saliente, o es parte de una sesión de comunicación ya establecida.

El problema del agotamiento de direcciones típicamente se maneja usando una técnica denominada traducción de dirección de red (NAT). La traducción de dirección de red se implementa comúnmente en conjunto con cortafuegos como parte de una disposición de seguridad de red global. La traducción de dirección de red permite que los dispositivos conectados a una red privada compartan una única dirección de IP. La idea básica detrás de la traducción de dirección de red es asignar la dirección privada de un espacio de direcciones privadas a dispositivos conectados a la red privada. Puesto que las direcciones privadas usan un espacio de direcciones diferente que la Internet pública, los paquetes que contienen una dirección privada no pueden encaminarse a través de la Internet. Para permitir que un dispositivo con una dirección de IP privada comunique con otros dispositivos en la Internet, un NAT (traductor de dirección de red) traduce direcciones de origen y destino privadas de paquetes válidos en el espacio de direcciones privadas a direcciones de origen y destino públicas válidas en el espacio de direcciones públicas.

Hay muchas diferentes implementaciones de NAT, que cada una afecta a protocolos de comunicación de capa superior de manera diferente. La presente invención trata problemas con el atravesamiento de las NAT simétricas, aunque la invención puede usarse con otros tipos de implementaciones de NAT. En una NAT simétrica, cada solicitud de la misma dirección y puerto de IP privados a una dirección y puerto de IP de destino específicos se mapea a una dirección y puerto de IP de origen público únicos. Si el mismo anfitrión interno envía un paquete de datos con la misma dirección y puerto de origen privados, pero a una dirección de IP o puerto públicos diferentes, se usa un mapeo diferente. En una NAT simétrica, los paquetes de datos enviados por un anfitrión externo se pasarán únicamente si el anfitrión interno ha invitado previamente una respuesta desde el anfitrión externo que envía el paquete de datos. Los paquetes de datos no invitados de un anfitrión externo se bloquearán por la NAT.

Aunque la traducción de dirección de red funciona bien con muchos protocolos comúnmente usados, tales como HTTP, POP y SMTP, puede crear problemas para algunos protocolos de comunicación de nivel de aplicación que envían direcciones de red explícitas en su carga útil. Por ejemplo, el Protocolo de Iniciación de Sesión (SIP) es un protocolo de señalización usado para establecer, mantener y terminar sesiones de voz sobre IP (VoIP). Una aplicación de VoIP típica usará diferentes direcciones y/o puertos para tráfico de señalización y tráfico de medios tal como tráfico de voz, vídeo y de fax. Para establecer la sesión de VoIP, el originador de la llamada invita a la parte llamada a participar en una llamada enviando una solicitud de Invitación de SIP (SIP INVITE). La parte llamada acepta la invitación enviando un mensaje de RESPUESTA de SIP (SIP RESPONSE). Los mensajes de Invitación de SIP y RESPUESTA de SIP típicamente incluyen direcciones y puertos específicos que se abren para el tráfico de RTP (medios).

En el caso donde la parte llamada esté detrás de una NAT simétrica, la solicitud de Invitación de SIP se bloqueará por la NAT y nunca alcanzará la parte llamada. Incluso si la parte llamada fuera alcanzable, la respuesta de SIP de la parte llamada se bloqueará en situaciones donde la parte llamante está detrás de un cortafuegos/NAT simétrico. Además, la aplicación de VoIP típicamente usará una dirección y puerto de IP diferentes para enviar y recibir tráfico de RTP o RCTP, por ejemplo, datos de voz. El cliente de VoIP no tiene manera de conocer la dirección externa asignada por la NAT para el tráfico de RTP y RTCP.

Se han usado un número de técnicas para resolver el problema de atravesamiento de NAT para comunicaciones de voz sobre IP. Una solución es usar una pasarela de nivel de aplicación (ALG). Una pasarela de nivel de aplicación es un componente de software que permite la examinación y modificación de paquetes de datos que pasan a través de la NAT. En el caso de paquetes de protocolo de SIP, la ALG puede sustituir direcciones de origen y destino privadas contenidas en la carga útil de mensajes de SIP con direcciones de origen y destino públicas. Esta técnica no asegura seguridad o autenticidad y es difícil desplegar puesto que la ALG debe tener conocimiento de los protocolos de nivel de aplicación. Por lo tanto, se requiere típicamente una ALG separada para cada aplicación.

Un protocolo de red denominado STUN (Utilidades de Atravesamiento de Sesión para NAT) descrito en el RFC 5389 permite que un dispositivo de anfitrión en una red privada descubra la presencia de un traductor de dirección de red y obtenga la dirección de NAT pública que se asignó para la conexión de UDP del usuario a un anfitrión remoto. Un dispositivo cliente genera y envía una solicitud de STUN a un servidor de aplicación en la red pública de STUN antes de establecer comunicación con un anfitrión remoto. La solicitud provoca que la NAT asigne una dirección pública y cree una vinculación entre la dirección pública y la dirección de origen privada de la solicitud de STUN. El servidor de aplicación STUN envía una respuesta de STUN al cliente y, dentro de su carga útil, devuelve la dirección de NAT pública asignada por la NAT. El cliente puede a continuación anunciar esta dirección pública como la dirección en la que recibirá paquetes de UDP (tanto para paquetes de señalización como de medios). El protocolo STUN no funciona con un cortafuegos simétrico en situaciones donde el cliente estará recibiendo paquetes de direcciones públicas distintas de la dirección pública del servidor de aplicación STUN.

Un protocolo denominado TURN (Atravesamiento Usando NAT de Retransmisión) proporciona una función de servidor de aplicación a un cliente detrás de una NAT para permitir que el cliente reciba datos entrantes a través de conexiones de TCP o UDP. Similar a STUN, un cliente envía una solicitud a un servidor de aplicación TURN antes de establecer comunicación con un anfitrión remoto. El servidor de aplicación TURN devuelve al cliente la dirección que puede usar como el destino para los medios, que el cliente usa como la dirección de destino para paquetes enviados al anfitrión remoto. La dirección de destino devuelta no es la dirección del anfitrión remoto, sino que en su lugar, es una dirección asociada con el servidor de aplicación TURN. El servidor de aplicación TURN actúa como un retransmisor y reenvía el paquete. Aunque TURN proporciona una solución al problema de atravesamiento de NAT, requiere que todos los paquetes se retransmitan por el servidor de aplicación TURN, y por lo tanto no es fácilmente escalable. Mientras que los retardos de red inducidos por la introducción de saltos de red adicionales típicamente no son suficientemente significativos para afectar la señalización de SIP, los paquetes de medios deberían entregarse con retardos mínimos. Por lo tanto, es preferible una solución que reduzca el número de saltos, y por lo tanto el retardo global.

Un controlador de borde de sesión (SBC) es un dispositivo usado en algunas redes de VoIP para atravesar un traductor de dirección de red. El SBC es un dispositivo a nivel de sesión que proporciona tanto funciones de control de intermediario de medios como de sesión. El SBC es esencialmente un intermediario que establece segmentos de llamada en dos diferentes redes. El SBC recibe paquetes en un segmento de llamada y los reenvía hacia el destino en el otro segmento de llamada. Debido a que el SBC modifica las direcciones, puede romper algunos mecanismos de seguridad. También, los controladores de borde de sesión son costosos, difíciles de desplegar, y no fácilmente escalables puesto que todos los paquetes deben retransmitirse a través del SBC.

Khlifi et al. “VoIP and NAT/Firewalls: Issues, Traversal Techniques, and a Real-World Solution”, IEEE Communications Magazine, IEEE Service Center, Piscataway, Estados Unidos, vol. N.° 44, n.º 7, 1 de julio de 2006, páginas 93-99, revisa diversas técnicas de atravesamiento de NAT y cortafuegos, y sugiere una solución que prevé el uso de un cliente de STUN, como un posible enfoque para proporcionar accesibilidad permanente a usuarios de VoIP.

Sumario

La presente invención proporciona un sistema y método para atravesamiento de una NAT simétrica para VoIP y otras sesiones de comunicación. El sistema y método usa cuatro componentes principales: un agente de retransmisión, un agente de NAT, un SIP proxy y un servidor de aplicación. El agente de retransmisión está localizado detrás del cortafuegos/NAT en una red privada y está configurado para comunicar con el SIP proxy localizado en la red pública. El agente de retransmisión encamina mensajes de señalización de SIP a través del SIP proxy. El servidor de aplicación solicita que el agente de retransmisión abra puertos de señalización en el cortafuegos/NAT para señalización entre el SIP proxy y el agente de retransmisión. El servidor de aplicación también solicita que los agentes de retransmisión abran puertos en el cortafuegos/NAT para tráfico de medios. El agente de NAT dispuesto en la ruta del cortafuegos/NAT a la Internet filtra paquetes de medios y cambia la dirección de origen pública de paquetes de medios entrantes a una dirección predeterminada asociada con el puerto de medios abierto.

La invención se define en las reivindicaciones independientes. Se proporcionan características adicionales de la invención en las reivindicaciones dependientes.

Breve descripción de los dibujos

La Figura 1 ilustra una red de comunicación ejemplar que incorpora un sistema de atravesamiento de NAT de acuerdo con una realización.

La Figura 2 ilustra los componentes principales de un sistema de atravesamiento de NAT de acuerdo con una invención ejemplar y el flujo de señal entre componentes.

La Figura 3 ilustra un procedimiento de registro usado para registrar un usuario con el servidor de aplicación y para abrir una conexión entre el servidor de aplicación y un agente de retransmisión.

La Figura 4 ilustra un procedimiento para mantener una conexión de señalización entre el servidor de aplicación de NAT y un agente de retransmisión.

Las Figuras 5A - 5D ilustran un procedimiento para establecer una sesión de comunicación a través de un cortafuegos de acuerdo con una realización ejemplar.

La Figura 6 ilustra un procedimiento para abrir una conexión de señalización o de medios a través de un cortafuegos.

La Figura 7 ilustra un procedimiento para mantener una conexión de señalización o de medios a través de un cortafuegos.

La Figura 8 ilustra reenvío de mensaje para tráfico de señalización en una realización de la invención.

La Figura 9 ilustra reenvío de mensaje para tráfico de medios en una realización de la invención.

La Figura 10 ilustra un encaminador en una realización alternativa.

Las Figuras 11A y 11B ilustran un procedimiento para establecer una sesión de comunicación a través de un cortafuegos de acuerdo con otra realización ejemplar.

La Figura 12 ilustra un dispositivo de anfitrión ejemplar para implementar componentes funcionales de la presente invención tales como el agente de retransmisión, agente de Nat, SIP proxy y servidor de aplicación.

Descripción detallada

Haciendo referencia ahora a los dibujos, la Figura 1 ilustra una red de comunicación 10 configurada de acuerdo con una realización ejemplar de la presente invención. La red de comunicación 10 comprende dos redes privadas 20 interconectadas con una red pública 40, tal como Internet. Para los fines de claridad, un número de referencia en la siguiente descripción puede ser seguido por cualquiera de la letra A para designar elementos asociados con la parte llamante, denominada en el presente documento como Usuario A, la letra B para designar elementos asociados con la parte llamada, denominada en el presente documento como Usuario B. Por lo tanto, la red privada 20A hace referencia a la red de la parte llamante, mientras que la red privada 20B hace referencia a la red privada de la parte llamada. Cuando se analizan elementos de manera genérica, el número de referencia puede usarse sin una letra. También, se observa que el término “dirección” como se usa en el presente documento hace referencia a una dirección de red completamente calificada que contiene tanto una dirección de IP como número de puerto. El término “dirección de IP” hace referencia a la dirección de red sin el número de puerto.

Cada red privada 20A, 20B incluye un cortafuegos/NAT 30A, 30B para proporcionar seguridad y proteger contra

acceso no autorizado a la red privada 20A, 20B. En esta realización, el cortafuegos/NAT 30A, 30B contiene hardware y/o software para implementar una NAT simétrica, aunque el uso de una NAT simétrica no es crucial para la invención. La presente invención puede usarse en conjunto con otras implementaciones de NAT.

Cada red 20A, 20B incluye una PBX (centralita privada) de IP (Protocolo de Internet) 50A, 50B que interconecta con la red telefónica pública conmutada (PSTN) y permite que se entreguen voz y datos a través de la PSTN. La PBX de IP 50A, 50B puede comprender cualquier pasarela de VoIP convencional que implemente protocolos de VoIP convencionales, tales como el Protocolo de Iniciación de Sesión (SIP) y RTP. La PBX de IP 50A, 50B puede usarse para establecer llamadas entre los usuarios 60A, 60B en las redes 20A, 20B a través de la red pública 40 en lugar de la PSTN. Como se describe en los antecedentes, la presencia del cortafuegos/NAT simétrico 30A, 30B en los límites de cada red privada 20A, 20B puede evitar que se establezca una sesión de voz sobre IP.

La red de comunicación 10 incluye un sistema 100 para atravesar el cortafuegos/NAT 30A, 30B para comunicaciones de VoIP como se muestra en la Figura 2. La presente invención podría aplicarse también en otras aplicaciones donde la información de dirección se lleve en la carga útil de paquetes de datos. El sistema 100 comprende cuatro tipos de componentes: agentes de retransmisión 110A, 110B que residen en las redes privadas 20A, 20B respectivamente, los agentes de NAT 120A, 120B que interceptan paquetes que llegan de la red pública 40 antes de que crucen el cortafuegos/NAT 30A, 30B respectivamente, un servidor de intermediario 130 en la red pública 40, y un servidor de aplicación 140 en la red pública 40. Los agentes de NAT 120A, 120B pueden desempeñar también un papel en abrir puertos en los cortafuegos 30A, 30B.

Los agentes de retransmisión 110A, 110B pueden implementarse como software en un dispositivo de anfitrión, por ejemplo, ordenador, en una red privada 20A, 20B. Los agentes de retransmisión 110A, 110B pueden residir, por ejemplo, en el mismo dispositivo anfitrión que la PBX de IP 50A, 50B, o pueden residir en un dispositivo anfitrión separado. Los agentes de retransmisión 110A, 110B podrían residir también en el equipo de usuario (UE). Los agentes de retransmisión 110A, 110B pueden funcionar en una disposición de agrupación para proporcionar una arquitectura tolerante a fallos.

El SIP proxy 130 y el servidor de aplicación 140 pueden implementarse como software en un ordenador conectado a la red pública 40. El SIP proxy 130 y el servidor de aplicación 140 pueden residir en el mismo ordenador, o en ordenadores separados. También, la funcionalidad del SIP proxy 130 y/o del servidor de aplicación 140 podría distribuirse entre varios ordenadores o procesadores, o en una agrupación de servidores de aplicación.

Los agentes de NAT 120A, 120B son esencialmente filtros de paquete con unas pocas funciones relativamente sencillas que pueden implementarse con software. Los agentes de retransmisión 110A, 110B y agentes de NAT 120A, 120B realizan unas pocas funciones relativamente sencillas, mientras que el volumen de la lógica está contenido en el SIP proxy 130 y el servidor de aplicación 140. Esta arquitectura proporciona una solución fácilmente escalable para atravesar un cortafuegos/NAT simétrico 30A, 30B.

Como se describirá en lo sucesivo en mayor detalle, los agentes de retransmisión 110A, 110B retransmiten señalización de SIP a y desde respectivas PBX de IP 50A, 50B. Los agentes de retransmisión 110A, 110B retransmiten paquetes de señalización salientes recibidos de las PBX de IP 50A, 50B al SIP proxy 130 en la red pública 40. De manera similar, los agentes de retransmisión 110A, 110B reciben paquetes de señalización de SIP desde el SIP proxy 130 en nombre de la respectiva PBX de IP 50A, 50B y retransmiten los mensajes de señalización de SIP entrantes a la PBX de IP 50A, 50B. El agente de retransmisión 110A, 110B no necesita analizar los contenidos de paquete para realizar la función de reenvío.

Los agentes de NAT 120A, 120B están dispuestos en la ruta de tráfico entre las redes privadas 20A, 20B y la red pública 40 e interceptan los paquetes entrantes antes de que crucen el cortafuegos de la red protegida 20A, 20B. En la realización mostrada en la Figura 1, el agente de NAT 120A intercepta paquetes de medios transmitidos por el Usuario B al Usuario A, mientras que el Agente de NAT 120B intercepta paquetes de medios transmitidos por el Usuario A al Usuario B. Los agentes de NAT 120A, 120B traducen direcciones de origen contenidas en los paquetes de medios para asegurar que las direcciones cumplen con políticas y reglas implementadas por los cortafuegos/NAT 30A, 30B.

El SIP proxy 130 y el servidor de aplicación 140 facilitan el establecimiento de la sesión de VoIP. Toda la señalización de SIP pasa a través del SIP proxy 130. El SIP proxy 130 recibe el mensaje de señalización de SIP desde el agente de retransmisión 110A o el agente de retransmisión 110B, modifica la información de dirección contenida en los mensajes de señalización de SIP, y reenvía los mensajes de señalización al agente de retransmisión 110B o al agente de retransmisión 110A.

El servidor de aplicación 140 comunica con el SIP proxy 130 y los agentes de retransmisión 110A, 110B en ambas redes privadas 20A, 20B. Se establece una conexión de TCP entre los agentes de retransmisión 110A, 110B y el servidor de aplicación 140, a través de los cortafuegos 30A, 30B. Esta conexión se mantiene abierta de modo que el servidor de aplicación 140 puede enviar solicitudes a los agentes de retransmisión 110A, 110B como se describirá en lo sucesivo. La función primaria del servidor de aplicación 140 es autorizar y facilitar sesiones de SIP y coordinar

con los agentes de retransmisión 110A, 110B para abrir puertos en los cortafuegos/NAT 30A, 30B tanto para tráfico de señalización como de medios, para obtener direcciones públicas asociadas con los puertos abiertos, y para proporcionar las direcciones de los puertos abiertos para señalización al SIP proxy 130.

Las Figuras 3-9 ilustran procedimientos ejemplares de acuerdo con una realización de la presente invención para atravesar un cortafuegos/NAT 30A, 30B usando una NAT simétrica. En este ejemplo, se supone que un usuario A en la red privada A está intentando establecer una llamada con un segundo usuario B en la red privada B. Se supone adicionalmente que tanto la red privada 20A como la red privada 20B incluyen un cortafuegos/NAT 30A, 30B que usa una NAT simétrica. Estas circunstancias son probablemente las más difíciles para atravesamiento de NAT. La presente invención puede usarse también cuando un cortafuegos/NAT está presente en únicamente un extremo de la comunicación, o con otros tipos de implementaciones de NAT. Por lo tanto, la realización ejemplar descrita en el presente documento no debería interpretarse como que limita la invención.

Para implementar el atravesamiento de NAT, los agentes de retransmisión 110A, 110B deben registrarse en primer lugar con el servidor de aplicación 140 y establecer un canal de comunicación con el servidor de aplicación 140. Se supone que ya se han establecido cuentas de usuario durante un procedimiento de suscripción. La Figura 3 ilustra un procedimiento de registro ejemplar. Para comenzar el procedimiento de registro, el agente de retransmisión 110A, 110B realiza un procedimiento de perforación de cortafuegos para descubrir la dirección de IP pública (natip) del cortafuegos/NAT 30A, 30B (etapa 1). El procedimiento de perforación de cortafuegos se describe en más detalle a continuación. Puesto que el agente de retransmisión 110A, 110B está únicamente interesado en descubrir la dirección de IP del cortafuegos/NAT 30A, 30B, no se mantiene la conexión abierta por el procedimiento de cortafuegos/perforación. El agente de retransmisión 110A, 110B almacena la dirección de IP del cortafuegos/NAT 30A, 30B. A continuación, el agente de retransmisión 110A, 110B abre uno o más puertos locales e inicia un procesador de intermediario que retransmite paquetes salientes recibidos en los puertos abiertos al SIP proxy 130 (etapa 2). Como un ejemplo, el agente de retransmisión 110A, 110B, puede elegir los puertos 5060 y 7000 para facilitar la integración con otros dispositivos de SIP. Para establecer una conexión de TCP con el servidor de aplicación 140, el agente de retransmisión 110A, 110B envía una solicitud de registro al servidor de aplicación 140 (etapa 3). La solicitud de registro incluye el ID de cuenta y contraseña para que se registre el usuario, la dirección de IP (natip) del cortafuegos/NAT 30A, 30B descubierto durante el procedimiento de perforación de cortafuegos, y la dirección privada en la que el agente de PBX 110A, 110B desearía recibir solicitudes de SIP.

Tras la recepción de la solicitud de registro saliente, el cortafuegos/NAT 30A, 30B asigna un puerto en el cortafuegos/NAT 30A, 30B y crea una entrada en su tabla de realización de NAT que asocia la dirección pública del puerto con la dirección privada del agente de retransmisión 110A, 110B desde la que se envió la solicitud de registro (etapa 4). El cortafuegos/NAT 30A, 30B, reenvía la solicitud de registro al servidor de aplicación 140 (etapa 5). Cuando el servidor 140 recibe la solicitud de registro, halla la cuenta especificada por el ID de cuenta y realiza autenticación usando la contraseña en la solicitud de registro. Si la autenticación es satisfactoria, el servidor de aplicación 140 almacena la dirección de origen pública de la solicitud de registro y la dirección de IP pública (natip) del cortafuegos/NAT 30A, 30B contenida en la solicitud de registro (etapa 6). El servidor de aplicación 140 envía una respuesta de registro al agente de retransmisión 110A, 110B para indicar que el registro fue satisfactorio (etapa 7).

Una vez que la conexión de TCP con el servidor de aplicación 140 está abierta, el agente de retransmisión 110A, 110B ejecuta periódicamente un procedimiento de mantenimiento de la conexión como se muestra en la Figura 4 para mantener la conexión de TCP con el servidor de aplicación 140. El procedimiento de mantenimiento de la conexión también asegura que el puerto en el cortafuegos/NAT 30A, 30B se mantiene abierto. El agente de retransmisión 110A, 110B envía un mensaje de mantenimiento de la conexión al servidor de aplicación 140 (etapa 1). El cortafuegos/NAT 30A, 30B intercepta el paquete, resetea el tiempo de vida para la conexión de TCP entre la dirección pública y privada del agente de retransmisión (etapa 2), y reenvía el mensaje de mantenimiento de la conexión al servidor de aplicación 140 (etapa 3). El mensaje de mantenimiento de la conexión indica al servidor de aplicación 140 que el agente de retransmisión 110A, 110B aún está disponible y que puede reenviarse la señalización para llamadas de VoIP al agente de retransmisión. El servidor de aplicación 140 puede enviar una respuesta de mantenimiento de la conexión para indicar al agente de retransmisión 110A, 110B que la conexión de TCP está aún abierta.

El servidor de aplicación 140 puede usar la conexión de TCP abierta durante el procedimiento de registro para enviar futuras solicitudes de perforación de cortafuegos al agente de retransmisión 110A, 110B para abrir puertos para conexiones de señalización y medios para sesiones de VoIP en el cortafuegos/NAT 30A, 30B como se describirá en lo sucesivo. Las conexiones de TCP entre los agentes de retransmisión 110A, 110B y el servidor de aplicación 140 pueden asegurarse usando transporte de SSL.

Las Figuras 5A - 5D ilustran un procedimiento ejemplar para establecer una llamada de VoIP entre el Usuario A y el Usuario B. Para proporcionar un ejemplo concreto, las direcciones de las entidades implicadas en la llamada serán como sigue:

Dirección privada del equipo de Usuario (para RTP)	192.168.1.200:24580
Dirección privada de la PBX de IP A	192.168.1.100:5060

Dirección privada del agente de retransmisión 110A	192.168.1.50:5060
Dirección privada del equipo del Usuario B (para RTP)	192.168.2.200:24582
Dirección privada de la PBX de IP B	192.168.2.100:5060
Dirección privada de agente de retransmisión 110B	192.168.2.50:5060
Dirección pública de SIP proxy 130	216.218.42.170:7000
Dirección pública de servidor de aplicación 140	216.218.42.170:8888

La dirección de IP pública si el cortafuegos/NAT 30A es 216.218.42.173 y la dirección de IP pública si el cortafuegos/NAT 30B es 216.218.42.172

El procedimiento comienza cuando el Usuario A (la parte llamante) inicia una llamada de VoIP llamando al número de teléfono público (por ejemplo, 514-666-1000) del Usuario B (etapa 1). Cuando la llamada se inicia, la PBX de IP A 50A genera una solicitud de Invitación de SIP y envía la solicitud de Invitación de SIP en un enlace troncal de SIP al agente de retransmisión 110A (etapa 2). La PBX de IP 50A para el Usuario A está configurada para usar un enlace troncal de SIP que apunta a la dirección del agente de retransmisión 110A. Una solicitud de Invitación de SIP ejemplar se proporciona a continuación.

```
INVITE sip:5146661000@dc.acme.com:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.100:5060;branch=z9hG4bK241f491779
Remote-Party-ID: <sip:1000@192.168.1.100>;party=calling;screen=yes;privacy=off
From: <sip:1000@192.168.1.100>;tag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-21178205
To: <sip:5146661000@dc.acme.com>
Date: Fri, 29 Jan 2010 20:10:13 GMT
Call-ID: 4dc24600-b63140a5-18-6401a8c0@192.168.1.100
Supported: timer,replaces
Min-SE:  1800
User-Agent: Cisco-CCM6.0
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, PUBLISH
CSeq: 101 INVITE
Contact: <sip:1000@192.168.1.100:5060>
Expires: 180
Allow-Events: presence, kpml
Session-Expires:  1800
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 214

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 192.168.1.100
s=SIP Call
c=IN IP4 192.168.1.200
t=0 0
m=audio 24580 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

En este punto, la línea de solicitud de la solicitud de Invitación de SIP contiene el URI de SIP del Usuario B (la parte llamada), y el campo de encabezamiento de CONTACTO y el campo de encabezamiento VÍA contiene la dirección privada la PBX de IP 50A. La descripción de medios contiene la dirección privada del equipo de usuario del Usuario A (UE A) para la conexión de medios.

El agente de retransmisión 110A recibe la solicitud de Invitación de SIP en el puerto 5060 y retransmite la solicitud de Invitación de SIP a la dirección pública (216.218.42.170:7000) del SIP proxy 130 en la red pública 40 (etapa 3). El agente de retransmisión 110A está configurado para retransmitir todos los paquetes recibidos en el puerto 5060 no modificados al SIP proxy 130. El cortafuegos/NAT 30A intercepta los paquetes salientes, cambia la dirección de origen de los paquetes a una dirección pública (216.218.42.173:cualquiera) del cortafuegos/NAT 30A, y reenvía el paquete al SIP proxy (etapa 4).

El SIP proxy 130 notifica al servidor de aplicación 140 que se ha recibido una nueva solicitud de Invitación de SIP desde el Usuario A (etapa 5). El servidor de aplicación 140 determina basándose en la dirección de origen del paquete que lleva la solicitud de Invitación de SIP que la solicitud de Invitación de SIP se origina desde un usuario en la red privada 20A puesto que la dirección de IP de origen de los paquetes coincide con la dirección obtenida por el servidor de aplicación 140 durante el registro (etapa 6). El servidor de aplicación 140 también determina que el

número de teléfono en el URI de solicitud corresponde a un número registrado asociado con la red privada 20B. (etapa 7).

Para posibilitar la sesión de VoIP, el servidor de aplicación 140 necesita abrir conexiones a través del cortafuegos/NAT 30A para la red privada 20A para tanto tráfico de señalización como de medios. Son necesarias dos conexiones de señalización y dos conexiones de medios en el lado llamante. Es necesaria una conexión de señalización para el CONTACTO especificado en la solicitud de Invitación de SIP original para posibilitar que la PBX de IP 50B envíe nuevas solicitudes de SIP. Es necesaria otra conexión de señalización para VÍA especificada en la Invitación de SIP original para posibilitar que la PBX de IP 50B envíe una respuesta a la Invitación de SIP. Ambas de las solicitudes y respuestas de SIP se enviarán a través del SIP proxy 130. Son necesarias también conexiones de medios separadas para tráfico de RTP y RTCP respectivamente.

Para abrir puertos en el cortafuegos/NAT 30A, el servidor de aplicación 140 envía una o más solicitudes de cortafuegos de perforación al agente de retransmisión 110A usando la conexión de TCP establecida durante el procedimiento de registro (etapa 8). Típicamente, el servidor de aplicación 140 enviará una solicitud de cortafuegos de perforación separada para cada conexión de señalización y de medios. Sin embargo, el procedimiento podría modificarse para permitir que se establezcan múltiples conexiones con una única solicitud de cortafuegos de perforación. Una solicitud de cortafuegos de perforación tiene un elemento de información (IE) para indicar el dispositivo objetivo de la solicitud de cortafuegos de perforación. El IE objetivo especifica la dirección pública (o dirección pública aparente) del dispositivo objetivo desde el que se enviarán los paquetes. La solicitud de cortafuegos de perforación también contiene un IE de destino, que especifica la dirección de destino privada de un dispositivo de destino al que se reenviarán los paquetes.

Para abrir una conexión para el CONTACTO, el servidor de aplicación 140 inserta la dirección pública (216.218.42.170:5060) del SIP proxy 130 en el IE objetivo y la dirección privada (192.168.1.100:5060) especificada en el campo de encabezamiento CONTACTO de la Invitación de SIP original en el IE de destino. Para abrir una conexión para VÍA, el servidor de aplicación 140 inserta la dirección pública (216.218.42.170:5060) del SIP proxy 130 en el IE objetivo y la dirección privada (192.168.1.100:5060) de la PBX de IP 50A especificada en campo de encabezamiento VÍA de la Invitación de SIP original en el IE de destino. Para las conexiones de RTP y RTCP, el servidor de aplicación 140 anexa el puerto 5353 a la dirección de IP (216.218.42.172) del cortafuegos/NAT 30B e inserta el resultado en el IE objetivo. La dirección creada es la dirección de origen pública aparente para paquetes de medios desde la parte llamada. Como se describirá en lo sucesivo, los paquetes de medios que llegan en el cortafuegos NAT 30A parecerá que se originan desde la dirección de origen pública aparente. Para las conexiones de RTP y RTCP, el servidor de aplicación 140 inserta la dirección privada (192.168.1.200:24580 para RTP y 192.168.1.200:24581 para RTCP) del teléfono de IP de la parte llamante en el IE de destino. La dirección privada del teléfono de IP de la parte llamante está contenida en el SDP de la solicitud de Invitación de SIP original.

En respuesta a cada solicitud de cortafuegos de perforación, el agente de retransmisión 110A implementa un procedimiento de perforación de cortafuegos descrito en más detalle a continuación para abrir un puerto para el dispositivo objetivo especificado por el servidor de aplicación 140 en el IE objetivo de la solicitud de cortafuegos de perforación. Durante el procedimiento de perforación de cortafuegos, agente de retransmisión 110A aprende la dirección pública abierta por el cortafuegos/NAT 30A. Después de que los puertos se han abierto para todas las conexiones solicitadas, el agente de retransmisión 110A informa las direcciones públicas de los puertos abiertos por el cortafuegos/NAT 30A al servidor de aplicación 140 en una o más respuestas de cortafuegos de perforación (etapa 9). En este ejemplo, se abren los siguientes puertos por el cortafuegos/NAT 30 A:

CONTACTO	216.218.42.173:2062
VÍA	216.218.42.173:2064
RTP	216.218.42.173:2066
RTCP	216.218.42.173:2068

Como se describirá en mayor detalle a continuación, el procedimiento de perforación de cortafuegos para las conexiones de RTP y RTCP también crea una entrada en la tabla de traducción para el agente de NAT 120A, que se usa para cambiar la dirección de origen de los paquetes de medios de la parte llamante que llegan al cortafuegos/NAT 30A.

El servidor de aplicación 140 también necesita abrir un puerto de cortafuegos en la red 20B y solicita que el agente de retransmisión 110B abra una conexión de señalización para señalización de SIP. Más específicamente, es necesario un puerto abierto en cortafuegos/NAT 30B para posibilitar que se entregue la solicitud de Invitación de SIP. La conexión de señalización se abre enviando una solicitud de cortafuegos de perforación desde el servidor de aplicación 140 al agente de retransmisión 110B (etapa 10). Como se ha descrito anteriormente, la solicitud de cortafuegos de perforación contiene un IE objetivo y un IE de destino. El servidor de aplicación 140 inserta la dirección (216.218.42.170:5060) del SIP proxy 130 en el IE objetivo para indicar que esos mensajes de señalización de SIP se enviarán desde la dirección pública del SIP proxy 130. El IE de destino contiene una dirección privada (192.168.2.100:5060) de la PBX de IP 50B. El procedimiento de perforación de cortafuegos posibilita que el agente de retransmisión 110B aprenda la dirección pública en el cortafuegos/NAT 30B abierto para la conexión de

señalización, que se devuelve en una respuesta de cortafuegos de perforación (etapa 11). En este ejemplo, la dirección devuelta para la conexión de señalización es 216.218.42.172:4811.

El servidor de aplicación 140 también solicita que el agente de retransmisión 110B reserve dos puertos para tráfico de RTP y RTCP saliente respectivamente. Para reservar puertos en el agente de retransmisión 110B, el servidor de aplicación 140 envía una solicitud de reserva de puerto al agente de retransmisión 110B (etapa 12). La solicitud de reserva de puerto incluye un IE de destino que indica las direcciones públicas abiertas por el cortafuegos/NAT 30A a las que se enviarán los paquetes de RTP y RTCP. En respuesta a la solicitud de reserva de puerto, el agente de retransmisión 110B reserva puertos para tráfico de RTP y RTCP saliente. El puerto reservado para tráfico de RTP saliente debería ser un puerto par, mientras que el puerto para RTCP es el siguiente puerto impar consecutivo. El agente de retransmisión 110B informa las direcciones privadas reservadas para el tráfico de RTP y RTCP al servidor de aplicación 140 en respuestas a las solicitudes de reserva de puerto (etapa 13). En este ejemplo, el agente de retransmisión 110B reserva 192.168.2.50:4814 para tráfico de RTP y 192.162.2.50:4815 para tráfico de RTCP.

En respuesta a la notificación desde el SIP proxy 130, el servidor de aplicación 140 devuelve las direcciones reservadas obtenidas al SIP proxy 130 (etapa 14) y el SIP proxy 130 modifica la solicitud de Invitación de SIP (etapa 15). Para una Invitación de SIP sencilla que contiene una descripción de medios de voz, se hacen las siguientes modificaciones a la Invitación de SIP:

1) El URI de solicitud se modifica de modo que contiene la extensión de teléfono privado para el UE B en la dirección de la PBX de IP privada. Esta dirección está configurada cuando se establece una cuenta en el servidor de aplicación 140.
2) La descripción de medios se modifica de modo que la dirección de RTP apunta a la dirección (192.168.2.50:4814) del agente de retransmisión 110B abierta para tráfico de RTP de modo que el tráfico de medios se enviará a través del agente de retransmisión.
3) Una primera ruta de registro que apunta a la dirección privada (192.168.1.50:7000) del agente de retransmisión 110A se añade de modo que futuras solicitudes de SIP desde la PBX de IP 50A en el mismo diálogo de SIP se enviarán a través del agente de retransmisión 110A.
4) Una segunda ruta de registro (en la parte superior de la anterior) que apunta a la dirección privada (192.168.2.50:7000) del agente de retransmisión 110B se añade de modo que futuras solicitudes de SIP desde la PBX de IP 50B dentro del mismo diálogo de SIP se enviarán a través del agente de retransmisión 110B.
5) Un VÍA más superior que apunta a la dirección pública (216.218.42.170:7000) del SIP proxy 130 se añade de modo que la respuesta de SIP se encamina a través del SIP proxy 130.

La solicitud de Invitación de SIP modificada con cambios destacados se muestra a continuación:

```
INVITE sip:1000@192.168.2.100:5060 SIP/2.0
Record-Route: <sip:192.168.2.50:7000;ftag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-
21178205;lr>
Record-Route: <sip:192.168.1.50:7000;ftag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-
21178205;lr>
Via: SIP/2.0/UDP 216.218.42.170:7000;branch=z9hG4bK241f491779
Via: SIP/2.0/UDP
192.168.1.100:5060;received=216.218.42.173;branch=z9hG4bK241f491779
Remote-Party-ID: <sip:1000@192.168.1.100>;party=calling;screen=yes;privacy=off
From: <sip:1000@192.168.1.100>;tag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-21178205
To: <sip:5146661000@dc.acme.com>
Date: Fri, 29 Jan 2010 20:10:13 GMT
Call-ID: 4dc24600-b63140a5-18-6401a8c0@192.168.1.100
Supported: timer,replaces
Min-SE:  1800
User-Agent: Cisco-CCM6.0
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, PUBLISH
CSeq: 101 INVITE
Contact: <sip:1000@192.168.1.100:5060>
Expires: 180
Allow-Events: presence, kpml
Session-Expires:  1800
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 211

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 192.168.1.100
```

```
s=SIP Call
c=IN IP4 192.168.2.50
t=0 0
m=audio 4814 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

El SIP proxy 130 envía la Invitación de SIP modificada a la dirección pública (216.218.42.172:4811) del puerto que se abrió en el cortafuegos/NAT 30B para recibir la Invitación de SIP (etapa 16). El procedimiento de perforación de cortafuegos previamente realizado por el agente de retransmisión 110B crea una vinculación para la dirección pública del puerto con la dirección privada del agente de retransmisión 110B. El cortafuegos/NAT 30B mapea la dirección de destino pública de la solicitud de Invitación de SIP a la dirección privada de agente de retransmisión 110B y reenvía la solicitud de Invitación de SIP al agente de retransmisión 110B en el puerto usado para enviar el FWPP en la etapa 10 (etapa 17). El agente de retransmisión 110B recibe la solicitud de Invitación de SIP modificada y reenvía la solicitud de Invitación de SIP a la PBX de IP 50B en 192.168.2.100:5060, que es la dirección especificada en el IE de destino de la solicitud de cortafuegos de perforación enviada en la etapa 10 (etapa 18). La PBX de IP 50B hace sonar el teléfono en la extensión 1000 (etapa 19). La PBX de IP 50B puede enviar una o más respuestas provisionales de SIP al SIP proxy 130 mientras espera que el Usuario B conteste.

Cuando el Usuario B contesta el teléfono, se envía una indicación a la PBX de IP 50B (etapa 20). La PBX de IP 50B acepta la solicitud de Invitación de SIP enviando una respuesta de SIP 200 OK con una descripción de medios a la dirección (216.218.42.170:7000) especificada en el VÍA más superior de la solicitud de Invitación de SIP. Esta es la dirección pública del SIP proxy 130. La respuesta SIP 200 OK se muestra a continuación:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 16.218.42.170:7000;branch=z9hG4bK241f491779;received=192.168.2.50
Via: IP/2.0/UDP192.168.1.100:5060;received=216.218.42.173;branch=z9hG4bK241f491779
From: <sip:1000@192.168.1.100>;tag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-21178205
To: <sip:5146661000@dc.acme.com>;tag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-26002145
Date: Fri, 29 Jan 2010 19:48:06 GMT
Call-ID: 4dc24600-b63140a5-18-6401a8c0@192.168.1.100
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, PUBLISH
Allow-Events: presence, kpml
Remote-Party-ID: <sip:1000@192.168.2.100>;party=called;screen=yes;privacy=off
Contact: <sip:1000@192.168.2.100:5060>

Record-Route: <sip:192.168.2.50:7000;ftag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-
21178205;lr>,<sip:192.168.1.50:7000;ftag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-
21178205;lr>
Supported: replaces
Session-Expires:  1800;refresher=uas
Require:  timer
Content-Type: application/sdp
Content-Length: 214

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 192.168.2.100
s=SIP Call
c=IN IP4 192.168.2.200
t=0 0
m=audio 24582 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

La descripción de medios de la respuesta SIP 200 OK contiene la dirección de IP (192.168.2.200) y el puerto (24582) del equipo de usuario (UE B) del Usuario B para la conexión de medios. El campo de encabezamiento CONTACTO contiene la dirección privada (192.168.2.100:5060) de la PBX de IP 50B.

La respuesta de SIP 220 OK se envía al agente de retransmisión (etapa 21). Tras la recepción de la respuesta de Invitación de SIP, el agente de retransmisión 110B retransmite la respuesta de Invitación de SIP (etapa 22). El cortafuegos/NAT 30B intercepta la respuesta SIP 200 OK y reenvía la respuesta al SIP proxy 130 (etapa 23). El SIP proxy 130 notifica al servidor de aplicación 140 que se recibió una respuesta SIP 200 OK para la transacción de SIP

(etapa 24).

En este punto, el servidor de aplicación 140 necesita abrir conexiones a través del cortafuegos/NAT 30B para tráfico de RTP y RTCP. También, es necesaria una conexión de señalización para posibilitar que la parte llamante envíe una solicitud de ACK de SIP que realiza acuse de recibo de la respuesta SIP 200 OK. El servidor de aplicación 140 envía una o más solicitudes de cortafuegos de perforación al agente de retransmisión 110B que indican que son necesarios puertos abiertos para tráfico de RTP y RTCP y para solicitudes de SIP (etapa 25). El IE objetivo de las solicitudes de cortafuegos de perforación para tanto tráfico de RTP como de RTCP contiene la dirección de IP del cortafuegos/NAT 30A con el número de puerto 5353 anexado. Esta es la dirección de origen pública aparente para paquetes de medios enviados por el Usuario A. Para la conexión de RTP, el IE de destino de la solicitud de cortafuegos de perforación contiene la dirección privada (192.168.2.200:24582) del teléfono del Usuario B para tráfico de RTP. Para la conexión de RTCP, el IE de destino de la solicitud de cortafuegos de perforación contiene la dirección privada (192.168.2.200:24583) del teléfono del Usuario B para tráfico de RTCP. Para abrir un puerto para solicitudes de SIP, el IE objetivo para la solicitud de cortafuegos de perforación es la dirección pública (216.218.42.170:7000) del SIP proxy 130 y el IE de destino es la dirección privada (192.168.2.100:5060) identificada en el campo de CONTACTO de encabezamiento de la respuesta SIP 200 OK. El agente de retransmisión 110B implementa el procedimiento de perforación de cortafuegos para abrir conexiones para tráfico de RTP y RTCP e informa las direcciones públicas abiertas para tráfico de RTP y RTCP respectivamente al servidor de aplicación 140 (etapa 26). En este ejemplo, la dirección pública para tráfico de RTP es 216.218.42.172:4816. La dirección pública para tráfico de RTCP es 216.218.42.172:4818. El agente de retransmisión 110B también informa la dirección pública abierta para la parte llamada CONTACTO, que en este ejemplo es 216.218.42.172:4812.

También es necesario que se reserven puertos por el agente de retransmisión 110A para tráfico de RTP y RTCP. El servidor de aplicación 140 envía solicitudes de reserva de puerto al agente de retransmisión 110A para reservar puertos en el agente de retransmisión 110A para tráfico de medios (etapa 27). Las solicitudes de reserva de puerto incluyen las direcciones públicas en el cortafuegos/NAT 30B devueltas en la etapa 26 en el IE de destino. En respuesta a las solicitudes de reserva de puerto, el agente de retransmisión 110A reserva dos puertos consecutivos para tráfico de RTP y RTCP respectivamente, y devuelve las direcciones privadas de los puertos reservados al servidor de aplicación 140 en una respuesta a las solicitudes de reserva de puerto (etapa 28). En este ejemplo, el puerto 2070 está reservado para RTP y el puerto 2071 está reservado para RTCP. El servidor de aplicación 140 retransmite las direcciones privadas al SIP proxy 130 para modificación de la respuesta de SIP (etapa 29).

El SIP proxy 130 modifica la respuesta de SIP para incluir información de dirección recibida desde el agente de retransmisión 110A (etapa 30). Más específicamente, el SIP proxy 130 elimina el VÍA más superior y modifica la descripción de medios de modo que la dirección de RTP apunta a la dirección (192.168.1.50:2070) del puerto reservado por el agente de retransmisión 110A para tráfico de RTP. La respuesta de SIP modificada 200 OK se muestra a continuación con cambios destacados:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 216.218.42.173:7000;branch=z9hG4bK241f491779;received=192.168.2.50
Via: SIP/2.0/UDP 192.168.1.100:5060;received=216.218.42.173;branch=z9hG4bK241f491779
From: <sip:1000@192.168.1.100>;tag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-21178205
To: <sip:5146661000@dc.acme.com>;tag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-26002145
Date: Fri, 29 Jan 2010 19:48:06 GMT
Call-ID: 4dc24600-b63140a5-18-6401a8c0@192.168.1.100
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, PUBLISH
Allow-Events: presence, kpml
Remote-Party-ID: <sip:1000@192.168.2.100>;party=called;screen=yes;privacy=off
Contact: <sip:1000@192.168.2.100:5060>
Record-Route: <sip:192.168.2.50:7000;ftag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-
21178205;lr>,<sip:192.168.1.50:7000;ftag=cfa850bf-a180-4e71-9b81-62d43df3a4f0-
21178205;lr>
Supported: replaces
Session-Expires:  1800;refresher=uas
Require:  timer
Content-Type: application/sdp
Content-Length: 211

v=0
o=CiscoSystemsCCM-SIP 2000 1 IN IP4 192.168.2.100
s=SIP Call
c=IN IP4 192.168.1.50
t=0 0
m=audio 2070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

El SIP proxy 130 envía la respuesta de SIP modificada 200 OK a la dirección pública (216.218.42.173:2064) para el puerto en el cortafuegos/NAT 30A que se abrió para la conexión VÍA (etapa 31). El procedimiento de perforación de cortafuegos previamente realizado por agente de retransmisión 110A creó una vinculación entre la dirección pública del puerto abierto por el cortafuegos/NAT 30A y la dirección privada en el agente de retransmisión 110A para la conexión de VÍA. Por lo tanto, el cortafuegos/NAT 30A traduce la dirección pública a la dirección privada del agente de retransmisión 110A y reenvía la respuesta al agente de retransmisión 110A (etapa 32). El agente de retransmisión 110A recibe la respuesta de SIP modificada 200 OK y, a su vez, reenvía la respuesta de SIP a la PBX de IP 50A en 192.168.1.100:5060, la dirección originalmente especificada en el encabezamiento VÍA de la solicitud de Invitación de SIP original (etapa 33).

La PBX de IP 50A procesa la respuesta de SIP (etapa 34). Para completar el diálogo de SIP, la PBX de IP 50A envía una solicitud de ACK de SIP al agente de retransmisión 110A (etapa 35). Puede observarse que en SIP, ACK es una solicitud y no una respuesta. Por lo tanto se envía a la dirección especificada en la primera ruta de registro, que se creó añadiendo una entrada de RUTA de REGISTRO en la Invitación de SIP que apunta al agente de retransmisión 110A. El agente de retransmisión 110A retransmite la solicitud de ACK de SIP al SIP proxy 130 (etapa 36). La NAT de cortafuegos 30A recibe la solicitud de ACK de SIP y la reenvía al SIP proxy (etapa 37). El SIP proxy 130 notifica al servidor de aplicación 140 que se recibió la solicitud de ACK (etapa 38). El servidor de aplicación 140 envía una respuesta al SIP proxy 130 que contiene la dirección en el agente de retransmisión 110B donde ha de enviarse la solicitud de ACK de SIP (etapa 39) El SIP proxy 130 retransmite la solicitud de ACK de SIP al agente de retransmisión 110B (etapa 40). El agente de retransmisión 110B a su vez reenvía la solicitud de ACK a la PBX de IP 50B (etapa 41). La PBX de IP 50B maneja la solicitud de ACK y se establece el diálogo (etapa 42). En este punto, existen puertos abiertos para conexiones de señalización y de medios en el cortafuegos/NAT 30A y 30B y se establece la llamada entre el Usuario A y el Usuario B.

La Figura 6 ilustra un procedimiento de perforación de cortafuegos para abrir conexiones a través de un cortafuegos. El procedimiento de perforación de cortafuegos se activa por el agente de retransmisión 110A, 110B en respuesta a un evento. Por ejemplo, el evento puede comprender una solicitud (por ejemplo, solicitud de cortafuegos de perforación desde el servidor de aplicación 140) para abrir un “agujero” en el cortafuegos/NAT corporativo 30A, 30B de modo que los paquetes que provengan desde un dispositivo objetivo en la Internet, se reenviaran a un dispositivo interno en la red privada (el dispositivo de destino). En el caso de una NAT simétrica, el agente de retransmisión 110A, 110B no puede abrir simplemente el agujero en nombre del dispositivo de destino; necesita permanecer en la ruta de los paquetes entrantes desde el dispositivo objetivo.

Para comenzar el procedimiento de perforación de cortafuegos, el agente de retransmisión 110A, 110B abre un conector y lo vincula a un puerto (etapa 1). El agente de retransmisión 110A, 110B envía un paquete especialmente formado denominado el paquete de perforación de cortafuegos (FWPP) desde el puerto abierto en la etapa 1 a la dirección de dispositivo objetivo (etapa 2). La dirección de origen del FWPP es la dirección del agente de retransmisión privada (agentip.agentport) desde la que se envía el FWPP y la dirección de destino del FWPP es la dirección de dispositivo objetivo (targetip.targetport). En el caso donde se inicie el procedimiento de perforación de cortafuegos en respuesta a una solicitud de cortafuegos de perforación desde el servidor de aplicación 140, la dirección de dispositivo objetivo es la dirección especificada en el IE objetivo de la solicitud de cortafuegos de perforación.

El cortafuegos/NAT corporativo 30A, 30B recibe el FWPP en el lado de la LAN y busca en su tabla de realización de NAT para observar si ya hay una asociación entre la dirección de origen privada del FWPP y la dirección de destino pública del FWPP (etapa 3). Si se halla una entrada coincidente, el cortafuegos/NAT 30A, 30B actualiza el tiempo de vida de esta entrada de realización de NAT y envía el FWPP a la dirección de destino pública usando la misma dirección de origen pública que se halló en la tabla. Si no se halla ninguna entrada coincidente, el cortafuegos/NAT 30A, 30B reserva una dirección de origen pública (*natip.natporf*) crea una nueva entrada en su tabla de realización de NAT que asocia la dirección de origen pública (*natip:natport*) con la dirección de agente de retransmisión (*agentip.agentport*) y la dirección de dispositivo objetivo (*targetip:targetport*), y envía el FWPP a la dirección de destino (*targetip.targetport*) desde la dirección de origen pública (*natip.natporf*) que acaba de reservar (etapa 4). El cortafuegos/NAT 30A, 30B ahora encamina cualquier paquete que llegue en *natip.natporf* desde *internetip* a *agentip.agentport*.

El agente de NAT 120A, 120B analiza cada paquete enviado desde el lado de la WAN del cortafuegos/NAT 30A, 30B al proveedor de servicio de Internet y puede reconocer fácilmente un FWPP. La mayoría de los paquetes excepto el FWPP (y unos pocos otros paquetes que se van a describir a continuación) se pasan sin modificar a través del agente de NAT 120A, 120B. El agente de NAT 120A, 120B, sin embargo, intercepta el FWPP y realiza la acción dependiendo de la dirección de dispositivo objetivo. Si la dirección de dispositivo objetivo incluye un puerto “fijo” predeterminado (puerto 5353 en este ejemplo), el agente de NAT 120A, 120B crea o actualiza una entrada en su tabla de traducción (etapa 5). La entrada comprende tres componentes: la dirección de origen pública (*natip.natporf*) del FWPP, la dirección de IP del dispositivo objetivo (*targetip*), y una indicación de tiempo que se usa para eliminar las entradas sin uso o caducadas. Para todos los FWPP, el agente de NAT 120A, 120B extrae la dirección de origen pública del FWPP y crea una respuesta de FWPP (FWPPR) (etapa 6). El FWPPR incluye en su carga útil la dirección de origen pública (*natip:natporf*) del FWPP, que es el puerto abierto en el cortafuegos/NAT

30A, 30B. El FWPP se descarta.

El agente de NAT 120A, 120B envía un FWPPR de vuelta a la dirección de origen pública (*natip.natport*) abierta por el FWPP (etapa 7). Cuando se crea el FWPPR, se intercambian la dirección de origen y de destino en el FWPP. El cortafuegos/NAT 30A, 30B recibe el FWPPR en la dirección pública abierta por el FWPP, traduce la dirección de destino pública del FWPPR a la dirección privada (*agentip.agentport*) del agente de retransmisión 110A, 110B (etapa 8), y reenvía el FWPPR al agente de retransmisión (etapa 9).

El agente de retransmisión 110A, 110B recibe el FWPPR en el puerto usado para enviar el FWPP (abierto en la etapa 1) y lee la dirección de origen pública contenida en la carga útil del FWPP (etapa 10). El agente de retransmisión 110A, 110B a continuación almacena la dirección pública devuelta en el FWPPR por el agente de NAT 120A, 120B. En este punto, el agente de retransmisión 110A, 110B conoce que si se ha enviado un paquete desde el dispositivo objetivo al cortafuegos/NAT 30A, 30B en *natip.natport*, se retransmitirá por el cortafuegos/NAT 30A, 30B al agente de retransmisión en agentip.agentport. El agente de retransmisión 110A, 110B mantiene el conector para esta conexión abierto y reenvía paquetes recibidos a través de este conector a un dispositivo de destino en la red privada. Cuando se solicita un puerto abierto por el servidor de aplicación, la dirección del dispositivo de destino se especifica en el IE de destino de la solicitud de cortafuegos de perforación y el agente de retransmisión 110A, 110B envía una respuesta de cortafuegos de perforación que contiene la dirección de origen pública (*natip.natport*) al servidor de aplicación 140.

El diseño del FWPP debería posibilitar que el agente de NAT 120A, 120B identifique rápidamente un FWPP. Para conseguir estos objetivos, el diseño del FWPP puede tener una longitud fija y comenzar con una firma predeterminada. También, el FWPP puede tener un formato predeterminado que posibilita análisis rápido. De manera similar, el FWPPR, está diseñado de modo que puede construirse fácilmente. Con este objetivo en mente, el FWPP está diseñado con algunos bytes sin uso que pueden usarse por el agente de NAT 120A, 120B para insertar la dirección de origen pública. El FWPP está diseñado para permitir que se intercambien rápidamente las direcciones de origen y destino. Además, el diseño de paquete permite que el agente de NAT 120A, 120B recalcule rápidamente una suma de comprobación para los encabezamientos de IP y UDP sin recalcular la suma de comprobación de la totalidad del paquete.

En una realización ejemplar, el FWPP es exactamente de 27 bytes de longitud. Los bytes 0-15 (16 bytes) contienen un identificador único (por ejemplo GUID). El byte 16 contiene un identificador de tipo de paquete que se establece a 01 para un FWPP y se establece a 02 para un FWPPR. Los bytes 17-20 (4 bytes) contienen un ID único secuencial generado por el agente de retransmisión 110A, 110B, usado para adaptar respuestas de FWPPR a solicitudes de FWPP y por lo tanto pueden descartarse respuestas a solicitudes antiguas. Los bytes 21-24 (4 bytes) se reservan para contener la dirección de IP pública abierta por el cortafuegos/NAT 30A, 30B en el paquete de FWPPR. Los bytes 26-27 (2 bytes) se reservan para contener el puerto público abierto por el cortafuegos/NAT 30A, 30B en el paquete de FWPPR.

Una vez que se ha realizado una apertura en el cortafuegos/NAT 30A, 30B, debería enviarse un mensaje de mantenimiento de la conexión al cortafuegos/NAT 30A, 30B de manera periódica para mantener el puerto abierto. La Figura 7 ilustra un procedimiento ejemplar para mantener un puerto abierto en la NAT/cortafuegos 30A, 30B. Cada pocos segundos, el agente de retransmisión 110A, 110B envía un mensaje de Mantenimiento de la Conexión de Cortafuegos (FWKA) al cortafuegos/NAT 30A, 30B (etapa 1). El mensaje de FWKA se envía a la misma dirección objetivo, y desde la misma dirección de origen que el FWPP anterior. El cortafuegos/NAT 30A, 30B halla la entrada existente en su tabla de vinculación que corresponde a la dirección de destino del FWKA y actualiza el tiempo de vida (etapa 2). El cortafuegos/NAT 30A, 30B envía el FWKA a la dirección de destino (etapa 3). El agente de NAT 120A, 120B intercepta el FWKA. Si la dirección de destino del paquete de FWKA es addrNATx:5353, el agente de NAT 120A, 120B actualizará el tiempo de vida para la correspondiente entrada en su tabla de traducción (etapa 4). El agente de NAT 120A, 120B a continuación descarta el FWKA (etapa 5).

En una realización ejemplar, el paquete de FWKA es de 17 bytes de longitud. Los bytes 0-15 (16 bytes) contienen un GUID (un identificador único). El byte 16 (1 byte) contiene un indicador de tipo de paquete (por ejemplo, 03 para indicar un FWKA).

La Figura 8 ilustra la ruta de mensajes de señalización de SIP después de que se hayan establecido conexiones de señalización de acuerdo con la presente invención. Los mensajes de señalización de SIP generados por la PBX de IP 50A, 50B se envían al agente de retransmisión local 110A, 110B (etapa 1). El agente de retransmisión local 110A, 110B reenvía el mensaje de señalización de SIP al SIP proxy 130 (etapa 2), que retransmite el mensaje a la dirección pública del puerto en el cortafuegos/NAT 30A, 30B abierto para la conexión de señalización (etapa 3). El cortafuegos/NAT 30A, 30B busca la correspondiente dirección privada en su tabla de vinculación (etapa 4). Como se ha observado previamente, la vinculación de la dirección pública con la dirección privada del agente de retransmisión remoto se creó durante el procedimiento de perforación de cortafuegos. El cortafuegos/NAT 30A, 30B reenvía el paquete al agente de retransmisión remoto 110A, 110B (etapa 5). El agente de retransmisión 110A, 110B también incluye una tabla de encaminamiento que asocia el puerto a través del cual se reciben mensajes de señalización de SIP con la dirección privada de la PBX de IP 50A, 50B. El agente de retransmisión 110A, 110B

busca la dirección interna asociada con el puerto de señalización (etapa 6), que es la dirección interna de la PBX de IP 50A, 50B. El agente de retransmisión 110A, 110B a continuación reenvía el mensaje de SIP a la PBX de IP remota (etapa 7).

La Figura 9 ilustra la ruta seguida por paquetes de RTP después de que se hayan establecido conexiones de medios. En este caso, se envían paquetes de RTP que se originan desde el equipo de usuario por el agente de retransmisión local 110A, 110B al agente de NAT del usuario remoto 120A, 120B (etapa 1). El agente de NAT del usuario remoto 120A, 120B incluye una tabla de traducción que asocia la dirección IP de origen pública y dirección de destino del paquete. El agente de NAT 120A, 120B cambia el puerto de origen del paquete a 5353 (etapa 2) y reenvía el paquete con la dirección de origen modificada al cortafuegos/NAT 30A, 30B (etapa 3). El cortafuegos/NAT 30A, 30B incluye una tabla de vinculación que asocia la dirección de destino pública del paquete con una dirección de destino privada. El cortafuegos/NAT 30A, 30B sustituye la dirección de destino pública con la dirección de destino privada en su tabla de vinculación (etapa 4) y reenvía el paquete al agente de retransmisión 110A, 110B (etapa 5). El agente de retransmisión 110A, 110B recuerda que los paquetes recibidos en un puerto específico necesitan reenviarse a otra dirección privada especificada en una solicitud de cortafuegos de perforación anterior (etapa 6). Esa dirección privada es la dirección privada del teléfono de IP del usuario. El agente de retransmisión remoto 110A, 110B sustituye la dirección privada del teléfono del usuario para la dirección de destino contenida en el paquete de datos y reenvía el paquete de datos al teléfono del usuario (etapa 7).

En otra realización ejemplar, la funcionalidad del agente de retransmisión 110A, 110B y del agente de NAT 120A, 120B pueden incorporarse en el encaminador 70A, 70B u otro dispositivo de anfitrión que implementa el cortafuegos/NAT 30A, 30B como se muestra en la Figura 10. En este caso, no habría necesidad de perforar el cortafuegos usando paquetes de FWPP/FWKA como se ha descrito anteriormente. En su lugar, el mismo encaminador 70A, 70B podría abrir las conexiones. El canal de comunicación entre el encaminador 70A, 70B y el servidor de aplicación 140 podría integrarse directamente en el código del encaminador para evitar el cortafuegos/NAT 30A, 30B. El encaminador 70A, 70B podría reservar uno o más puertos (por ejemplo, puerto 5060) para reenviar tráfico de SIP interno al servidor de aplicación 140. El encaminador 70A, 70B, podría configurarse mediante una interfaz de explorador como es conocido en la técnica.

Cuando se activa un encaminador 70A, 70B que contiene el agente de retransmisión 110A, 110B y el agente de Nat 120A, 120B implementaría un procedimiento de arranque y establecería una conexión con el servidor de aplicación 140. Durante el procedimiento de arranque, el encaminador 70A, 70B reserva un puerto (por ejemplo, puerto 5060) en el lado de red interna para retransmitir tráfico al servidor de aplicación 140. Esta dirección de encaminador privada puede configurarse como un enlace troncal de SIP en la PBX de IP 50A, 50B. El encaminador 70A, 70B conecta con el servidor de aplicación 140 usando opcionalmente un protocolo seguro, tal como CORBA a través de SSL, usando una conexión directamente en el lado de la WAN del encaminador 70A, 70B, eliminando por lo tanto la necesidad de atravesamiento de NAT. La función del agente de retransmisión 110A, 110B en el encaminador 70A, 70B enviaría aún señales de mantenimiento de la conexión al servidor de aplicación 140 para mantener la conexión de TCP con el servidor de aplicación 140. Cuando el servidor de aplicación 140 requiere aperturas de puerto en el cortafuegos/NAT 30A, 30B, la función de agente de retransmisión 110A, 110B en el encaminador 70A, 70B podría iniciar actualizaciones de la tabla de realización de NAT del encaminador directamente de modo que se reenvían paquetes de señalización de SIP entrantes directamente a la PBX de IP 50A, 50B.

El requisito de contigüidad de puerto de RTP/RTCP puede tratarse directamente en el código del encaminador 70A, 70B teniendo el cortafuegos/NAT 30A, 30B que reservar dos puertos públicos consecutivos para conexiones de RTP y RTCP. Por lo tanto, no hay necesidad de que el agente de retransmisión 110A, 110B en el extremo remoto funcione como un intermediario saliente para tráfico de RTP y RTCP. En un sistema mixto donde un extremo usa un encaminador 70A, 70B con el agente de retransmisión integrado 110A, 110B y el agente de NAT 120A, 120B, y el otro extremo tenga un agente de retransmisión separado 110A, 110B y agente de NAT 120A, 120B, el servidor de aplicación 140 podría detectar que los puertos públicos en el extremo con un sistema integrado son consecutivos y por lo tanto evitar crear los puertos de intermediario en el agente de retransmisión 110A, 110B en el otro extremo. En este caso, el servidor de aplicación 140 podría dirigir los paquetes de medios para que se envíen directamente a través de la Internet en lugar de encaminarlos a través del agente de retransmisión 110A, 110B.

La necesidad de un tratamiento especial de tráfico de medios entrante aún está presente, pero la solución es diferente. El servidor de aplicación 140 podría simplemente solicitar que el encaminador 70A, 70B reserve un puerto público y encamine tráfico en ese puerto que proviene desde una dirección de IP específica (la dirección de cortafuegos remota) al punto de extremo de medios en la red privada 20A, 20B. Por lo tanto se elimina la necesidad de modificar el número de puerto de paquetes de medios entrantes.

La Figura 11 ilustra un procedimiento ejemplar para atravesar un cortafuegos en el escenario donde la funcionalidad del agente de retransmisión 110A, 110B y del agente de NAT 120A, 120B, y del cortafuegos/NAT 30A, 30B está contenida en un encaminador 70A, 70B. El procedimiento comienza cuando el Usuario A inicia una llamada marcando el número de teléfono del Usuario B (etapa 1). La PBX de IP 50A para el Usuario A genera una solicitud de Invitación de SIP y envía la solicitud de Invitación de SIP en un enlace troncal de SIP al encaminador 70A (etapa 2). El encaminador 70A reenvía la solicitud de Invitación de SIP al SIP proxy 130 (etapa 3). El SIP proxy 130 notifica

al servidor de aplicación 140 que se ha realizado una nueva llamada (etapa 4). El servidor de aplicación 140 determina la identidad del Usuario A (etapa 5) y del Usuario B (etapa 6) desde los contenidos de la solicitud de Invitación de SIP como se ha descrito anteriormente. El servidor de aplicación 140 a continuación envía una solicitud al encaminador 70A para abrir puertos para conexiones de señalización y de medios (etapa 7). Se requieren cuatro puertos: uno para el CONTACTO en la solicitud de Invitación de SIP, uno para el VÍA en la solicitud de Invitación de SIP, uno para RTP, y uno para RTCP como se ha descrito anteriormente. El encaminador 70A abre puertos en el cortafuegos (etapa 8) y devuelve las direcciones de los puertos al servidor de aplicación 140 (etapa 9).

El servidor de aplicación 140 a continuación solicita que el encaminador 70B abra un puerto para la solicitud de Invitación de SIP (etapa 10). El encaminador 70B abre un puerto (etapa 11) y devuelve la dirección del puerto al servidor de aplicación (etapa 12). El servidor de aplicación 140 a continuación devuelve valores al SIP proxy 130 para modificar la Invitación de SIP (etapa 13). El SIP proxy 130 modifica la Invitación de SIP (etapa 14) y envía la Invitación de SIP modificada al puerto abierto por el encaminador 70B (etapa 15). El encaminador 70B reenvía la Invitación de SIP modificada a la PBX de IP 50B (etapa 16) que hace sonar la extensión telefónica del Usuario B (etapa 17).

Cuando el Usuario B contesta (etapa 18), la PBX de IP 50B envía una respuesta de SIP OK al encaminador 70B (etapa 19). El encaminador 70B reenvía el SIP OK al SIP proxy 130 (etapa 20). El SIP proxy 130 notifica al servidor de aplicación 140 que se ha recibido una respuesta de SIP OK (etapa 21). El servidor de aplicación 140 a continuación envía una solicitud al encaminador 70B para abrir puertos para conexiones de RTP y RTCP y para una conexión de señalización adicional para un acuse de recibo del mensaje de respuesta de SIP (etapa 22). El encaminador 70B abre los puertos para RTP y RTCP (etapa 23) y devuelve las direcciones al servidor de aplicación 140 (etapa 24). El servidor de aplicación 140 devuelve valores al SIP proxy 130 para modificar la repuesta de SIP OK (etapa 25). El SIP proxy 130 modifica la respuesta de SIP OK (etapa 26) y envía la respuesta de SIP OK modificada al encaminador 70A. El encaminador 70A reenvía la respuesta de SIP OK modificada a la PBX de IP 50A (etapa 28). Aunque no se muestra en la Figura 11, la PBX de IP 50A envía una solicitud de ACK de SIP para establecer el diálogo de SIP.

La Figura 12 ilustra un dispositivo de anfitrión ejemplar 200 para implementar componentes funcionales de la presente invención tales como el agente de retransmisión 110A, 110B, el agente de NAT 120A, 120B, el SIP proxy 130, el servidor de aplicación 140, y el encaminador 70A, 70B. El dispositivo anfitrión 200 comprende una o más interfaces de red 206 para conectar el dispositivo anfitrión con una red privada, una red pública, o ambas, un procesador 204 para implementar los procedimientos descritos en el presente documento, y una memoria 202 para almacenar código de programa y datos para implementar los procedimientos descritos en el presente documento. El procesador 204 puede comprender uno o más microprocesadores, hardware, o una combinación de los mismos. La memoria 202 puede comprender tanto memoria volátil (por ejemplo, RAM) para datos de almacenamiento temporal y memoria no volátil (por ejemplo ROM, EEPROM) para almacenar código de programa y datos de configuración.

La presente invención puede llevarse a cabo, por supuesto, en otras maneras específicas distintas a aquellas expuestas sin alejarse del alcance de la invención según se reivindica.

REIVINDICACIONES

1. Un método de atravesamiento de un cortafuegos (30A) de traducción de dirección de red (NAT) en una red privada (20A) de una parte llamante, comprendiendo dicho método:
recibir, por un SIP proxy (130) en una red pública (40), una solicitud de Invitación de SIP desde una parte llamante;
enviar una primera solicitud de cortafuegos de perforación a un agente de retransmisión (110A), detrás del cortafuegos, para que la parte llamante abra un puerto en el cortafuegos (30A) para enviar mensajes de señalización de SIP desde el SIP proxy (130), conteniendo la solicitud de cortafuegos de perforación una dirección pública para el SIP proxy (130) y una dirección de SIP privada de la parte llamante obtenida desde la solicitud de Invitación de SIP;
recibir un primer mensaje de respuesta de perforación desde el agente de retransmisión (110A), conteniendo el primer mensaje de respuesta de perforación la dirección pública de un puerto en el cortafuegos (30A) abierto para mensajes de señalización de SIP desde el SIP proxy (130);
reenviar la solicitud de Invitación de SIP desde el SIP proxy (130) a la parte llamada;
recibir un mensaje de respuesta de SIP en respuesta a la solicitud de Invitación de SIP en el SIP proxy (130); y
reenviar el mensaje de respuesta de SIP desde el SIP proxy (130) a la dirección pública del puerto abierto para mensajes de señalización de SIP.

2. El método de la reivindicación 1, que comprende adicionalmente modificar la Invitación de SIP antes de reenviar la Invitación de SIP a la parte llamada para asegurar que se envía la señalización de SIP desde la parte llamada en el mismo diálogo de SIP a la parte llamante a través del SIP proxy (130).

3. El método de la reivindicación 2, en el que modificar la Invitación de SIP antes de reenviar la Invitación de SIP desde el SIP proxy (130) a la dirección predeterminada asociada con la parte llamada comprende:
añadir la dirección pública del SIP proxy (130) como la dirección más superior a un campo de encabezamiento Via de modo que el mensaje de respuesta de SIP se encaminará al SIP proxy (130);
añadir una primera ruta de registro que contiene una dirección del agente de retransmisión (110A) para la parte llamante a la solicitud de Invitación de SIP de modo que se enviarán posteriores solicitudes de SIP desde la parte llamante en el mismo diálogo de SIP a través del agente de retransmisión (110A) para la parte llamante;
si la parte llamada está en una red pública (40), añadir una segunda ruta de registro que contiene una dirección del SIP proxy (130) a la solicitud de Invitación de SIP de modo que se enviarán nuevas solicitudes de SIP desde la parte llamada a través del SIP proxy (130); y
si la parte llamada está en una red privada (20B), añadir una segunda ruta de registro que contiene una dirección del agente de retransmisión (110B) de la parte llamada a la solicitud de Invitación de SIP de modo que se enviarán nuevas solicitudes de SIP desde la parte llamada a través de un agente de retransmisión (110B) para la parte llamada,
opcionalmente en el que modificar la Invitación de SIP antes de reenviar la Invitación de SIP desde el SIP proxy (130) a la dirección predeterminada asociada con la parte llamada comprende adicionalmente modificar un URI de solicitud de la solicitud de Invitación de SIP para hacer coincidir el URI de destino de la parte llamada.

4. El método de una cualquiera de las reivindicaciones 1 a 3, que comprende adicionalmente:
enviar una segunda solicitud de cortafuegos de perforación a un agente de retransmisión (110A) para que la parte llamante abra un puerto de cortafuegos para recibir paquetes de medios desde la parte llamada, conteniendo la segunda solicitud de cortafuegos de perforación una dirección de origen pública aparente para paquetes de medios enviados por dicha parte llamada;
recibir un segundo mensaje de respuesta de perforación desde el agente de retransmisión (110A) para la parte llamante, conteniendo el segundo mensaje de respuesta de perforación una dirección pública de un puerto en el cortafuegos (30A) abierto para recibir paquetes de medios desde la parte llamada,
y/o que comprende adicionalmente:
enviar una o más solicitudes de reserva de puerto a un agente de retransmisión (110B) para que la parte llamada reserve uno o más puertos para recibir paquetes de medios desde la parte llamada, incluyendo cada solicitud de reserva de puerto una dirección de destino de la parte llamante para retransmitir paquetes de medios desde la parte llamada; y
recibir una o más respuestas de reserva de puerto desde un agente de retransmisión (110B) para la parte llamada en respuesta a la solicitud de reserva de puerto, conteniendo cada respuesta de reserva de puerto una dirección de un puerto reservado.

5. El método de la reivindicación 4, que comprende adicionalmente modificar una descripción de medios en la solicitud de Invitación de SIP antes de reenviar la solicitud de Invitación de SIP de modo que una dirección de destino para la conexión de medios es:
una dirección de intermediario en un agente de retransmisión (110A) para la parte llamante;
o una dirección pública de un puerto en el cortafuegos (30A) abierto para recibir paquetes de medios desde la parte llamada.

6. Un método de atravesamiento de un cortafuegos (30B) de traducción de dirección de red (NAT) en una red (20B) de una parte llamada, que comprende:
recibir, por un SIP proxy (130) en una red pública (40), una solicitud de Invitación de SIP desde una parte llamante;

enviar desde un servidor de aplicación (140) una primera solicitud de cortafuegos de perforación a un agente de retransmisión (110B), detrás del cortafuegos, para que la parte llamada abra un puerto de cortafuegos para enviar la solicitud de Invitación de SIP desde el SIP proxy (130), conteniendo la primera solicitud de cortafuegos de perforación una dirección pública para el SIP proxy (130) y una dirección privada para la parte llamada previamente registrada con el servidor de aplicación (140);
recibir un primer mensaje de respuesta de perforación desde el agente de retransmisión (110B) para la parte llamada, conteniendo el primer mensaje de respuesta de perforación la dirección pública del puerto en el cortafuegos (30B) abierto para la solicitud de Invitación de SIP desde el SIP proxy (130);
reenviar la solicitud de Invitación de SIP desde el SIP proxy (130) a la parte llamada enviando la solicitud de Invitación de SIP a la dirección pública del puerto de cortafuegos abierto para la solicitud de Invitación de SIP,
recibir, en el SIP proxy (130), un mensaje de Respuesta de SIP desde la parte llamada en respuesta a la solicitud de Invitación de SIP; y
reenviar el mensaje de Respuesta de SIP desde el SIP proxy (130) a la parte llamante.

7. El método de la reivindicación 6, que comprende adicionalmente modificar la Invitación de SIP antes de reenviar la Invitación de SIP desde el SIP proxy (130) a la dirección predeterminada asociada con la parte llamada para asegurar que esos mensajes de señalización de SIP desde la parte llamada en el mismo diálogo de SIP se envían a la parte llamante a través del SIP proxy (130), en el que modificar la solicitud de Invitación de SIP comprende:
añadir la dirección pública del SIP proxy (130) como la dirección más superior a un campo de encabezamiento Via de modo que el mensaje de respuesta de SIP se encaminará al SIP proxy (130);
si la parte llamante está localizada en una red pública (40), añadir una primera ruta de registro que contiene una dirección del SIP proxy (130) a la solicitud de Invitación de SIP de modo que se enviarán posteriores solicitudes de SIP desde la parte llamante en el mismo diálogo de SIP a través del intermediario de SIP (130); y
si la parte llamante está localizada en una segunda red privada (20A), añadir una primera ruta de registro que contiene una dirección de un agente de retransmisión (110A) para la parte llamante a la solicitud de Invitación de SIP de modo que se enviarán posteriores solicitudes de SIP desde la parte llamante en el mismo diálogo de SIP a través del agente de retransmisión (110A) para la parte llamante;
añadir una segunda ruta de registro que contiene una dirección del agente de retransmisión (110B) para la parte llamada a la solicitud de Invitación de SIP de modo que se enviarán nuevas solicitudes de SIP desde la parte llamada a través del agente de retransmisión (110B) para la parte llamada.

8. El método de la reivindicación 6 o 7, que comprende adicionalmente:
enviar una segunda solicitud de cortafuegos de perforación a un agente de retransmisión (110B) para que la parte llamada abra uno o más puertos de cortafuegos para recibir paquetes de medios desde la parte llamante, conteniendo la segunda solicitud de cortafuegos de perforación una dirección de origen pública aparente para paquetes de medios enviados por la parte llamante;
recibir un segundo mensaje de respuesta de perforación desde un agente de retransmisión (110B) para la parte llamada, conteniendo el segundo mensaje de respuesta de perforación la dirección o direcciones públicas del puerto o puertos de cortafuegos en el cortafuegos (30B) abierto para recibir paquetes de medios desde la parte llamante,
y/o que comprende adicionalmente:
enviar una o más solicitudes de reserva de puerto al agente de retransmisión (110A) para que la parte llamante reserve uno o más puertos para recibir paquetes de medios desde la parte llamante, incluyendo cada solicitud de reserva de puerto una dirección de destino para que la parte llamada retransmita paquetes de medios desde la parte llamante; y
recibir una o más respuestas de reserva de puerto desde el agente de retransmisión (110A) para la parte llamante en respuesta a las solicitudes de reserva de puerto, conteniendo cada respuesta de reserva de puerto una dirección de un puerto reservado.

9. El método de una cualquiera de las reivindicaciones 6 a 8, que comprende adicionalmente modificar una descripción de medios en Respuesta de SIP antes de reenviar el mensaje de Respuesta de SIP desde el SIP proxy (130) al agente de retransmisión (110B) de modo que la dirección de destino para una conexión de medios es:
una dirección de intermediario en el agente de retransmisión (110A) asociado con la parte llamante;
o una dirección pública de un puerto en el cortafuegos (30B) abierto para recibir paquetes de medios desde la parte llamante,
y/o que comprende adicionalmente:
enviar una tercera solicitud de cortafuegos de perforación al agente de retransmisión (110B) para que la parte llamada abra un puerto de cortafuegos para enviar mensajes de señalización de SIP desde el SIP proxy (130), conteniendo la tercera solicitud de cortafuegos de perforación una dirección pública para el SIP proxy (130) y una dirección privada para la parte llamada obtenidas desde el mensaje de Respuesta de SIP; y
recibir un tercer mensaje de respuesta de perforación desde el agente de retransmisión (110B) para la parte llamada, conteniendo el tercer mensaje de respuesta de perforación la dirección pública del puerto en el cortafuegos (30B) abierto para mensajes de señalización de SIP desde el SIP proxy (130).

10. Un sistema para atravesar un cortafuegos (30A) de traducción de dirección de red (NAT) en una red privada (20A) de una parte llamante, comprendiendo dicho sistema:
un SIP proxy (130) configurado para:

recibir una solicitud de Invitación de SIP desde una parte llamante y para reenviar la solicitud de Invitación de SIP desde el SIP proxy (130) a la parte llamada;
recibir un mensaje de respuesta de SIP desde la parte llamada en respuesta a la solicitud de Invitación de SIP en el SIP proxy (130) y reenviar el mensaje de respuesta de SIP desde el SIP proxy (130) a la parte llamante; y
un servidor de aplicación (140) configurado para:
enviar una primera solicitud de cortafuegos de perforación a un agente de retransmisión (110A), detrás del cortafuegos, para que la parte llamante abra un puerto en el cortafuegos (30A) para enviar mensajes de señalización de SIP desde el SIP proxy (130) a la parte llamante, conteniendo la solicitud de cortafuegos de perforación una dirección pública para el SIP proxy (130) y una dirección privada de la parte llamante obtenida desde la solicitud de Invitación de SIP; y
recibir un primer mensaje de respuesta de perforación desde el agente de retransmisión (110A), conteniendo el primer mensaje de respuesta de perforación una dirección pública de un puerto en el cortafuegos (30A) abierto para mensajes de señalización de SIP desde el SIP proxy (130),
en el que el SIP proxy está configurado para reenviar el mensaje de respuesta de SIP recibido desde la parte llamada a la dirección pública del puerto abierto para mensajes de señalización de SIP.

11. Un sistema de atravesamiento de cortafuegos (30B) de traducción de dirección de red (NAT) en una red (20B) de una parte llamada, que comprende:
un SIP proxy (130) configurado para:
recibir una solicitud de Invitación de SIP desde una parte llamante;
reenviar la solicitud de Invitación de SIP desde el SIP proxy (130) a la parte llamada enviando la solicitud de Invitación de SIP a la dirección pública del puerto de cortafuegos abierto para la solicitud de Invitación de SIP;
recibir un mensaje de Respuesta de SIP desde la parte llamada en respuesta a la solicitud de Invitación de SIP; y
reenviar el mensaje de Respuesta de SIP desde el SIP proxy (130) a la dirección pública del puerto abierto para mensajes de señalización de SIP; y
un servidor de aplicación (140) configurado para:
enviar una primera solicitud de cortafuegos de perforación a un agente de retransmisión (110B), detrás del cortafuegos, para que la parte llamada abra un puerto de cortafuegos para enviar la solicitud de Invitación de SIP desde el SIP proxy (130), conteniendo la primera solicitud de cortafuegos de perforación una dirección pública para el SIP proxy (130) y una dirección privada para la parte llamada previamente registrada con el servidor de aplicación (140); y
recibir un primer mensaje de respuesta de perforación desde el agente de retransmisión (110B) para la parte llamada, conteniendo el primer mensaje de respuesta de perforación la dirección pública del puerto en el cortafuegos (30B) abierto para la solicitud de Invitación de SIP desde el SIP proxy (130).

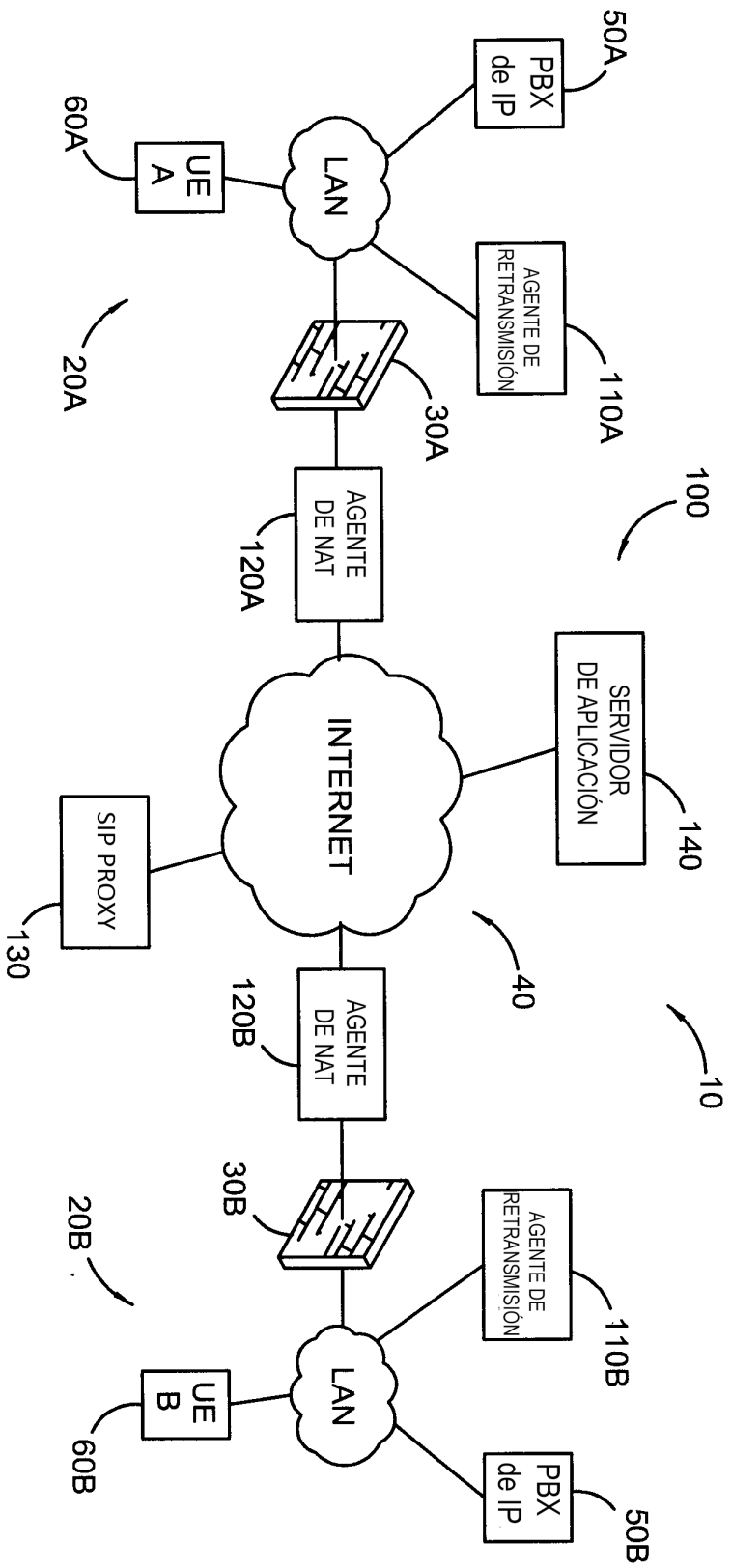
50A
PBX de IP
60A
UE A
LAN
AGENTE DE RETRANSMISIÓN
110A
20A
30A
AGENTE DE NAT
120A
100
SERVIDOR DE APLICACIÓN
140
INTERNET
SIP PROXY
130
40
120B
AGENTE DE NAT
10
30B
AGENTE DE RETRANSMISIÓN
110B
20B
LAN
UE B
60B
PBX de IP
50B

FIG. 1

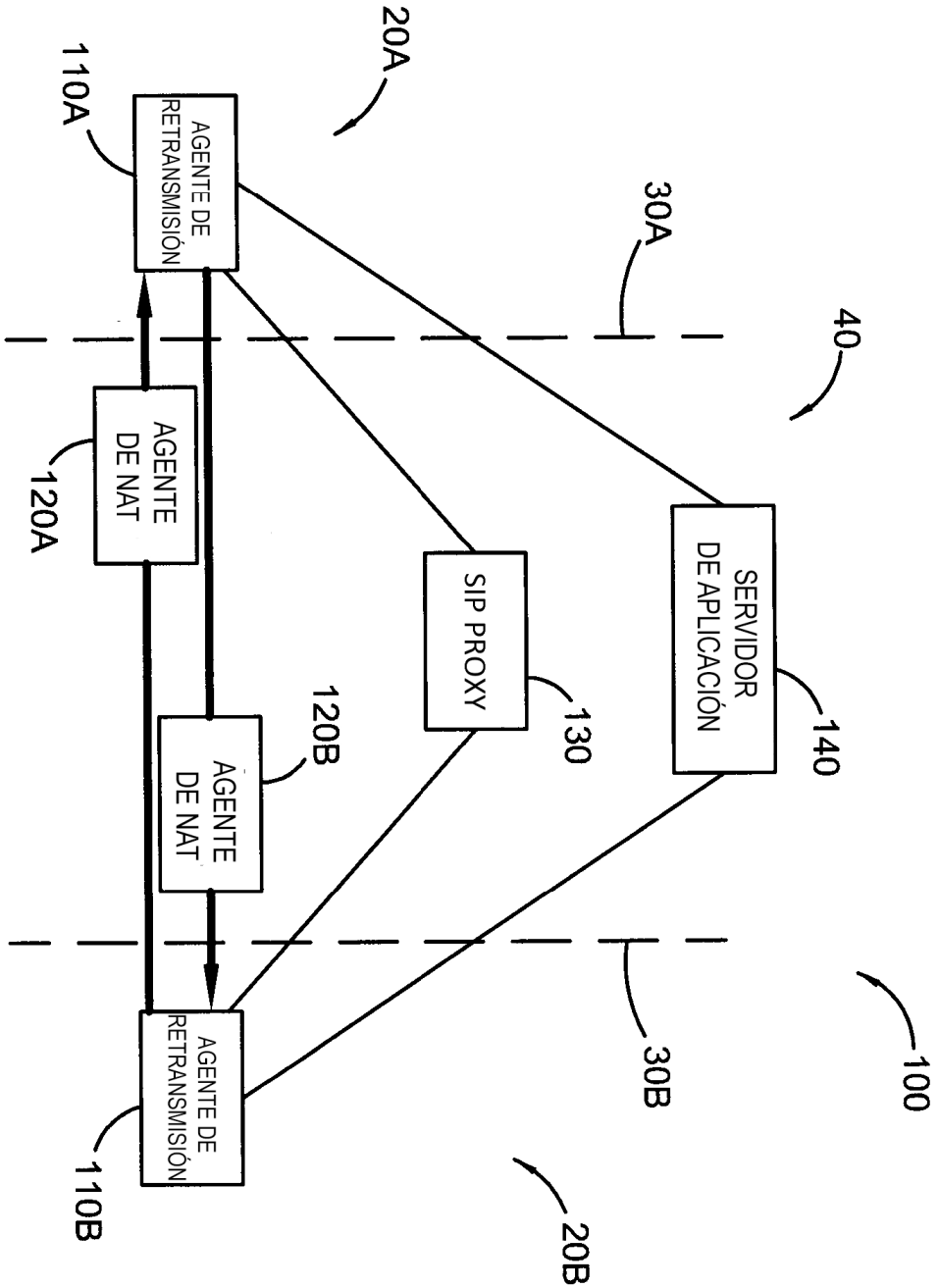
20A
110A
AGENTE DE RETRANSMISIÓN
30A
40
AGENTE DE NAT
120A
SIP PROXY
130
SERVIDOR DE APLICACIÓN
140
120B
AGENTE DE NAT
30B
100
AGENTE DE RETRANSMISIÓN
110B
20B

FIG. 2

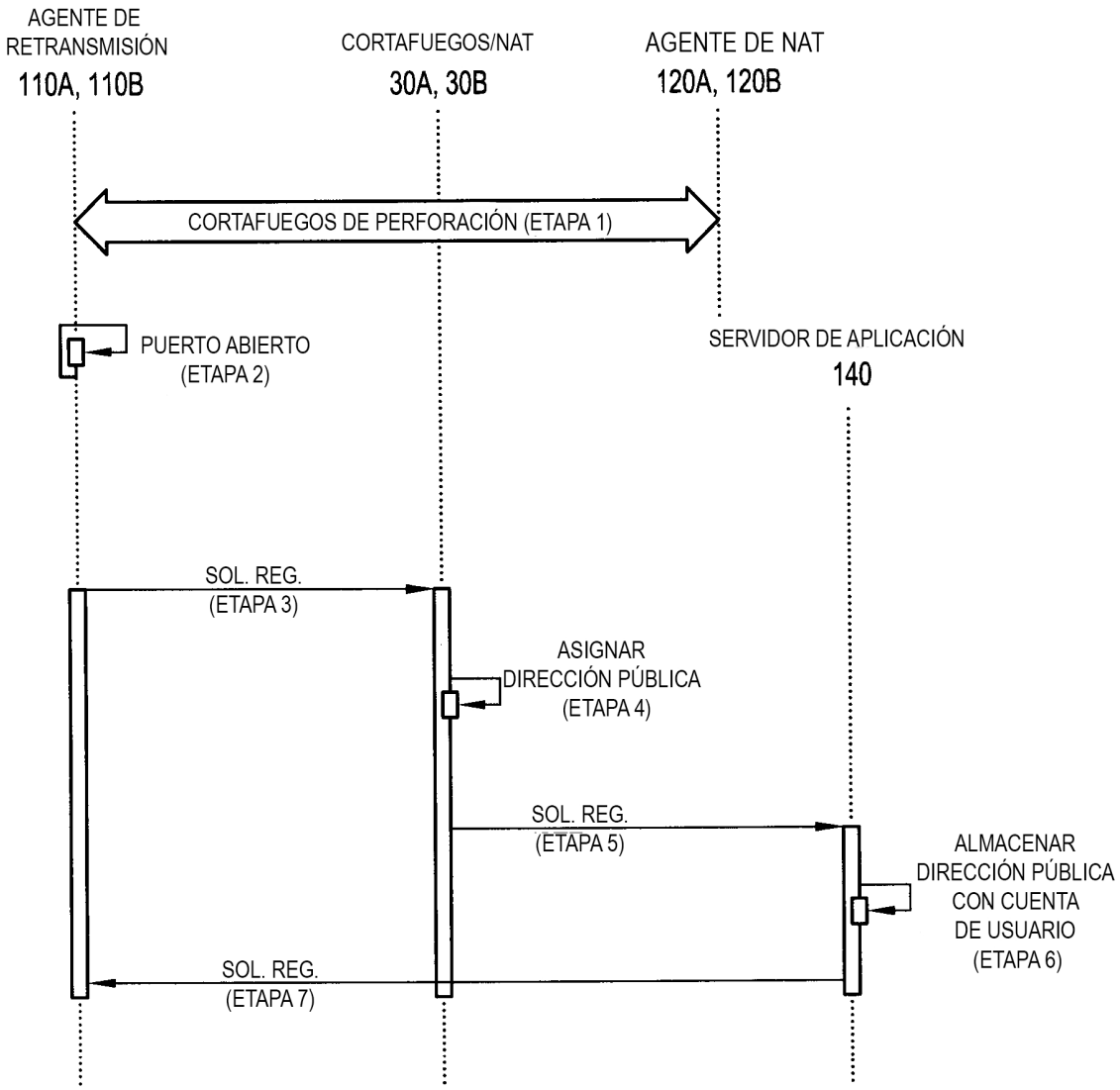
AGENTE DE RETRANSMISIÓN
110A, 110B
CORTAFUEGOS/NAT
30A, 30B
AGENTE DE NAT
120A, 120B
CORTAFUEGOS DE PERFORACIÓN (ETAPA 1)
PUERTO ABIERTO (ETAPA 2)
SERVIDOR DE APLICACIÓN
140
SOL. REG. (ETAPA 3)
ASIGNAR DIRECCIÓN PÚBLICA (ETAPA 4)
SOL. REG. (ETAPA 5)
ALMACENAR DIRECCIÓN PÚBLICA CON CUENTA DE USUARIO (ETAPA 6)
SOL. REG. (ETAPA 7)

FIG. 3

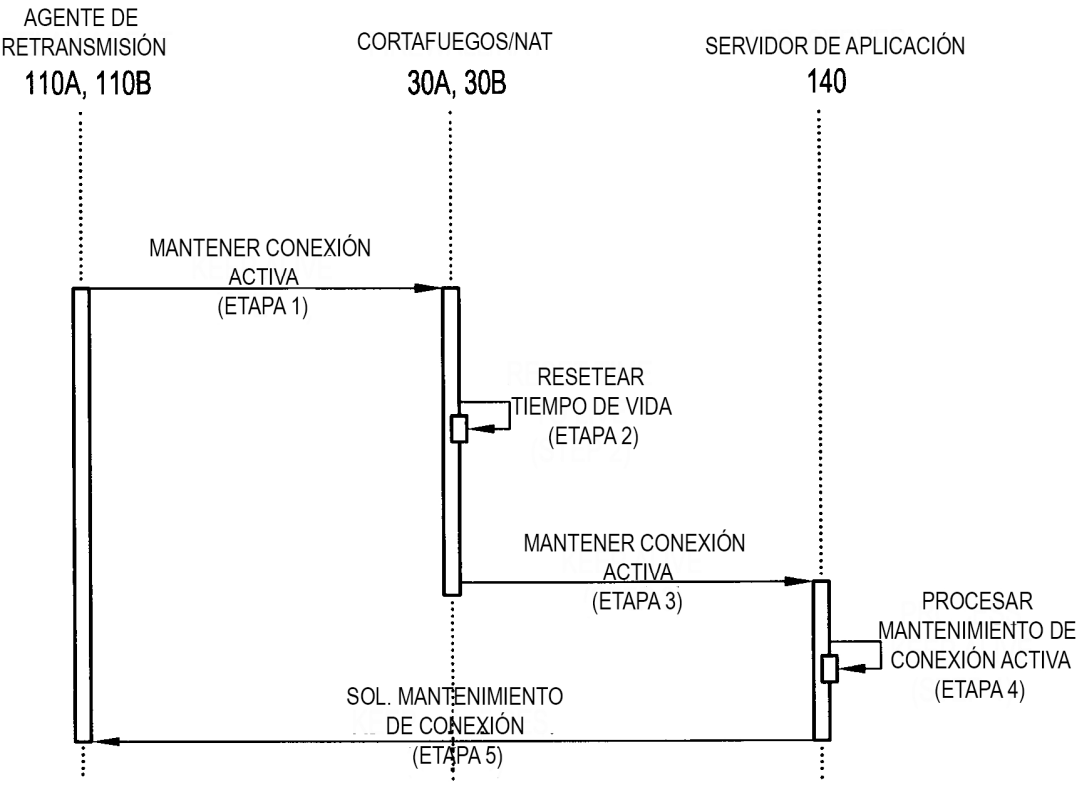
AGENTE DE RETRANSMISIÓN
110A, 110B
CORTAFUEGOS/NAT
30A, 30B
SERVIDOR DE APLICACIÓN
140
MANTENER CONEXIÓN ACTIVA (ETAPA 1)
RESETEAR TIEMPO DE VIDA (ETAPA 2)
MANTENER CONEXIÓN ACTIVA (ETAPA 3)
PROCESAR MANTENIMIENTO DE CONEXIÓN ACTIVA (ETAPA 4)
SOL. MANTENIMIENTO DE CONEXIÓN (ETAPA 5)

FIG. 4

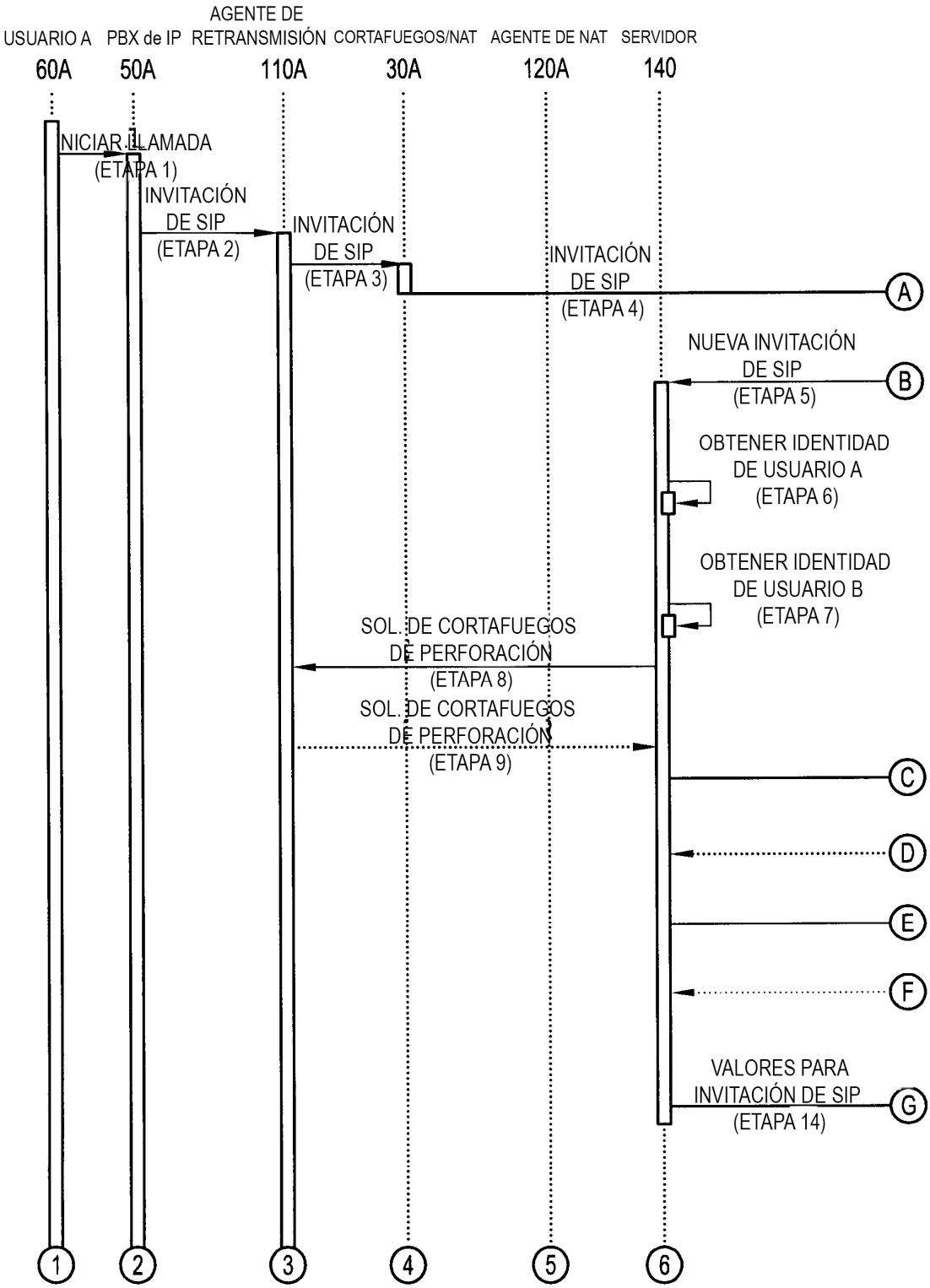
USUARIO A
PBX de IP
AGENTE DE RETRANSMISIÓN
CORTAFUEGOS/NAT
AGENTE DE NAT
SERVIDOR
60A
50A
110A
30A
120A
140
INICIAR LLAMADA (ETAPA 1)
INVITACIÓN DE SIP (ETAPA 2)
INVITACIÓN DE SIP (ETAPA 3)
INVITACIÓN DE SIP (ETAPA 4)
A
NUEVA INVITACIÓN DE SIP (ETAPA 5)
B
OBTENER IDENTIDAD DE USUARIO A (ETAPA 6)
OBTENER IDENTIDAD DE USUARIO B (ETAPA 7)
SOL. DE CORTAFUEGOS DE PERFORACIÓN (ETAPA 8)
SOL. DE CORTAFUEGOS DE PERFORACIÓN (ETAPA 9)
C
D
E
F
VALORES PARA INVITACIÓN DE SIP (ETAPA 14)
G
1
2
3
4
5
6

FIG. 5A

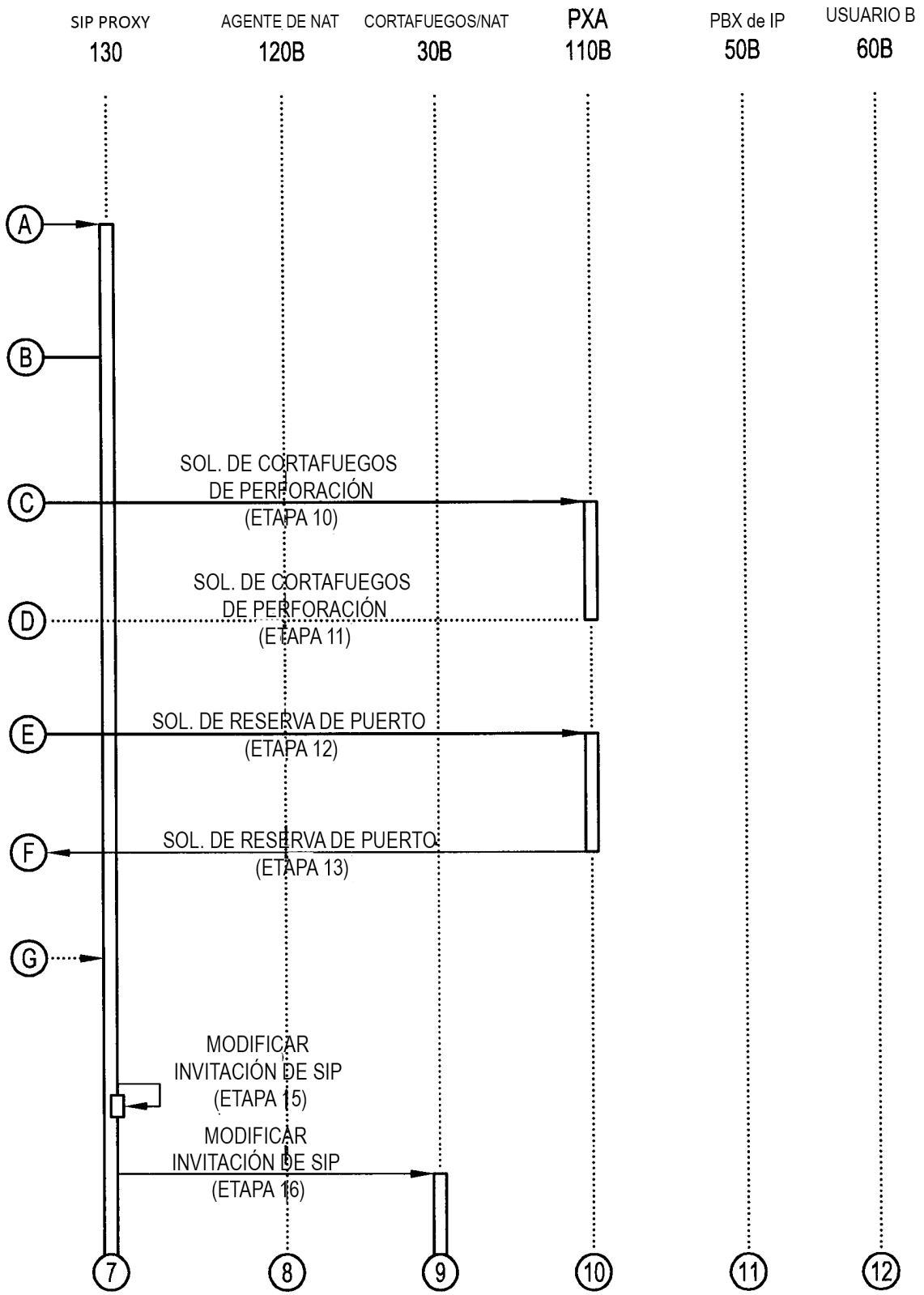
SIP PROXY
130
AGENTE DE NAT
120B
CORTAFUEGOS/NAT
30B
PXA
110B
PBX de IP
50B
USUARIO B
60B
A
B
C
SOL. DE CORTAFUEGOS DE PERFORACIÓN (ETAPA 10)
D
SOL. DE CORTAFUEGOS DE PERFORACIÓN (ETAPA 11)
E
SOL. DE RESERVA DE PUERTO (ETAPA 12)
F
SOL. DE RESERVA DE PUERTO (ETAPA 13)
G
MODIFICAR INVITACIÓN DE SIP (ETAPA 15)
MODIFICAR INVITACIÓN DE SIP (ETAPA 16)
7
8
9
10
11
12

FIG. 5B

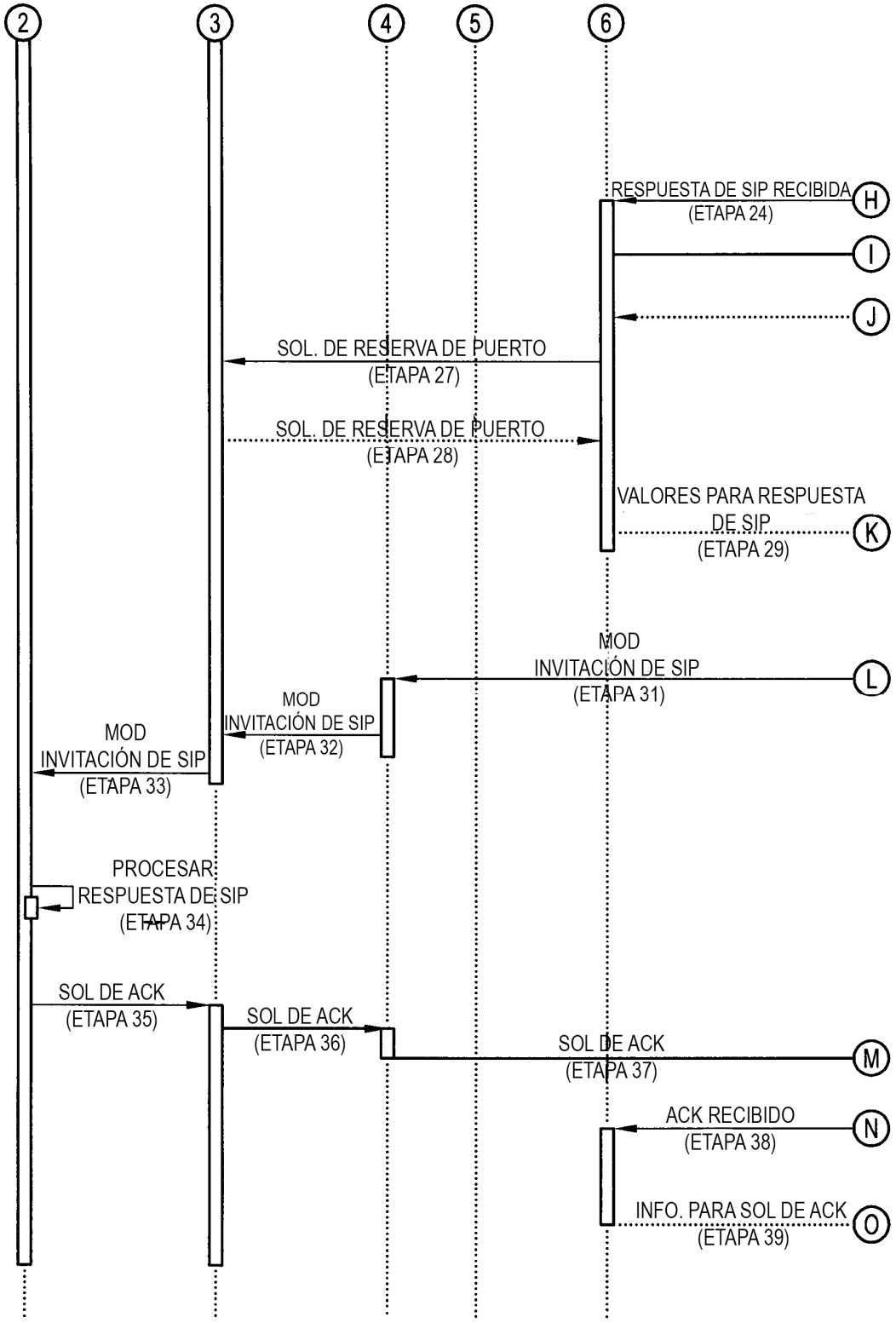
2
3
4
5
6
RESPUESTA DE SIP RECIBIDA
(ETAPA 24)
H
I
J
SOL. DE RESERVA DE PUERTO
(ETAPA 27)
SOL. DE RESERVA DE PUERTO
(ETAPA 28)
VALORES PARA RESPUESTA
DE SIP
(ETAPA 29)
K
MOD
INVITACIÓN DE SIP
(ETAPA 31)
L
MOD
INVITACIÓN DE SIP
(ETAPA 32)
MOD
INVITACIÓN DE SIP
(ETAPA 33)
PROCESAR
RESPUESTA DE SIP
(ETAPA 34)
SOL DE ACK
(ETAPA 35)
SOL DE ACK
(ETAPA 36)
SOL DE ACK
(ETAPA 37)
M
ACK RECIBIDO
(ETAPA 38)
N
INFO. PARA SOL DE ACK
(ETAPA 39)
O

FIG. 5C

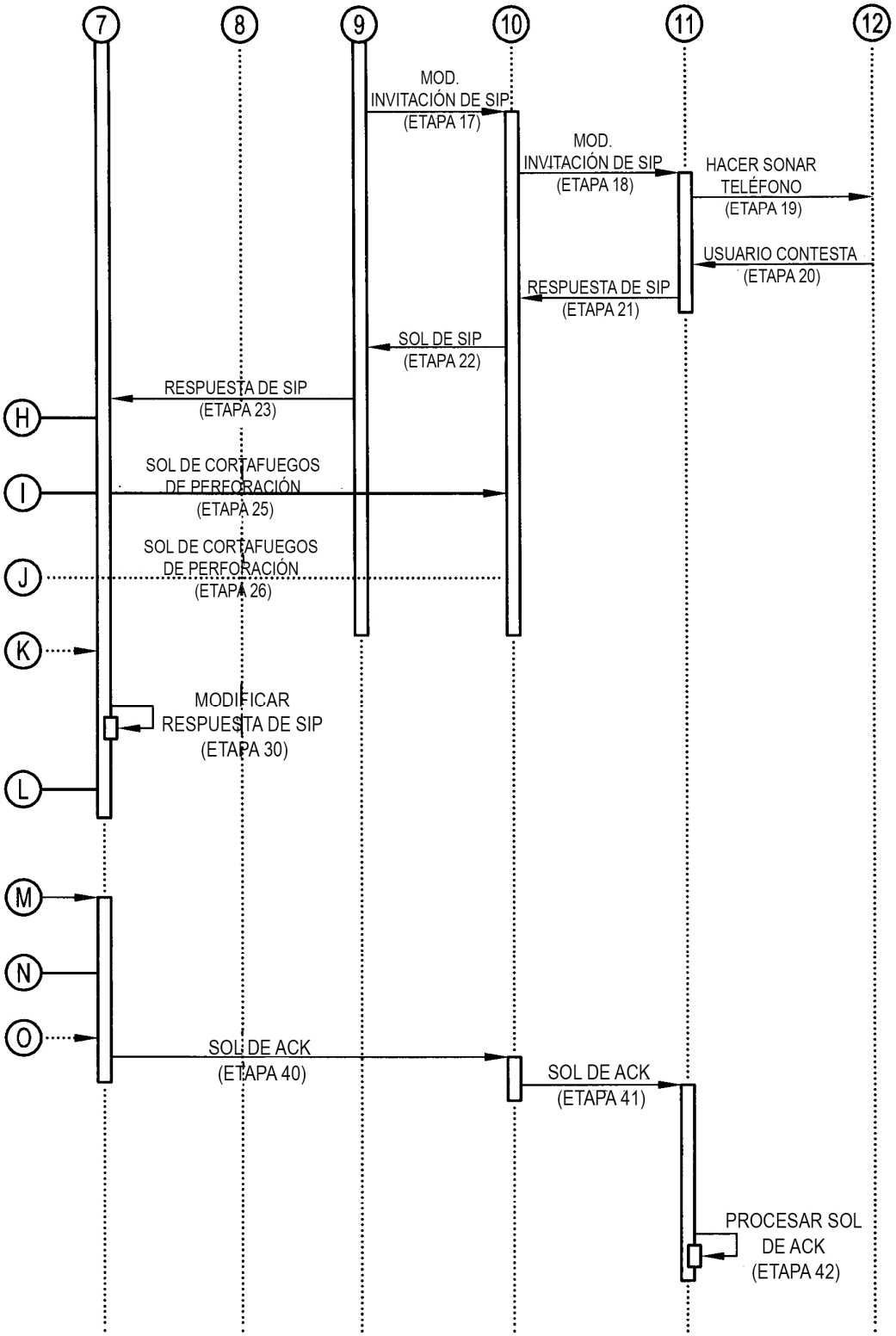
7
8
9
10
11
12
MOD.
INVITACIÓN DE SIP
(ETAPA 17)
MOD.
INVITACIÓN DE SIP
(ETAPA 18)
HACER SONAR
TELÉFONO
(ETAPA 19)
USUARIO CONTESTA
(ETAPA 20)
RESPUESTA DE SIP
(ETAPA 21)
SOL DE SIP
(ETAPA 22)
RESPUESTA DE SIP
(ETAPA 23)
H
I
SOL DE CORTAFUEGOS
DE PERFORACIÓN
(ETAPA 25)
J
SOL DE CORTAFUEGOS
DE PERFORACIÓN
(ETAPA 26)
K
MODIFICAR
RESPUESTA DE SIP
(ETAPA 30)
L
M
N
O
SOL DE ACK
(ETAPA 40)
SOL DE ACK
(ETAPA 41)
PROCESAR SOL
DE ACK
(ETAPA 42)

FIG. 5D

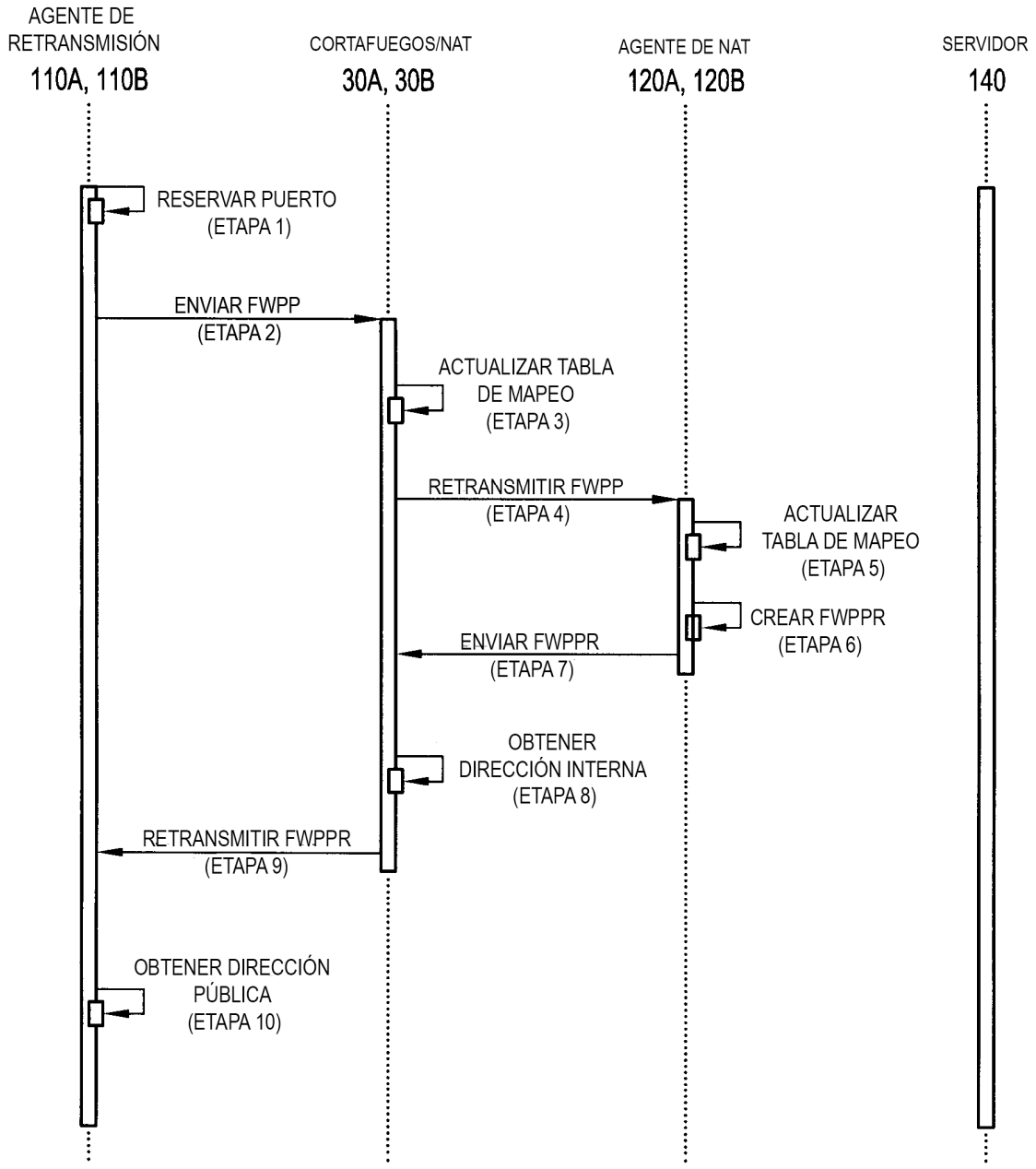
AGENTE DE RETRANSMISIÓN
110A, 110B
CORTAFUEGOS/NAT
30A, 30B
AGENTE DE NAT
120A, 120B
SERVIDOR
140
RESERVAR PUERTO
(ETAPA 1)
ENVIAR FWPP
(ETAPA 2)
ACTUALIZAR TABLA DE MAPEO
(ETAPA 3)
RETRANSMITIR FWPP
(ETAPA 4)
ACTUALIZAR TABLA DE MAPEO
(ETAPA 5)
CREAR FWPPR
(ETAPA 6)
ENVIAR FWPPR
(ETAPA 7)
OBTENER DIRECCIÓN INTERNA
(ETAPA 8)
RETRANSMITIR FWPPR
(ETAPA 9)
OBTENER DIRECCIÓN PÚBLICA
(ETAPA 10)

FIG. 6

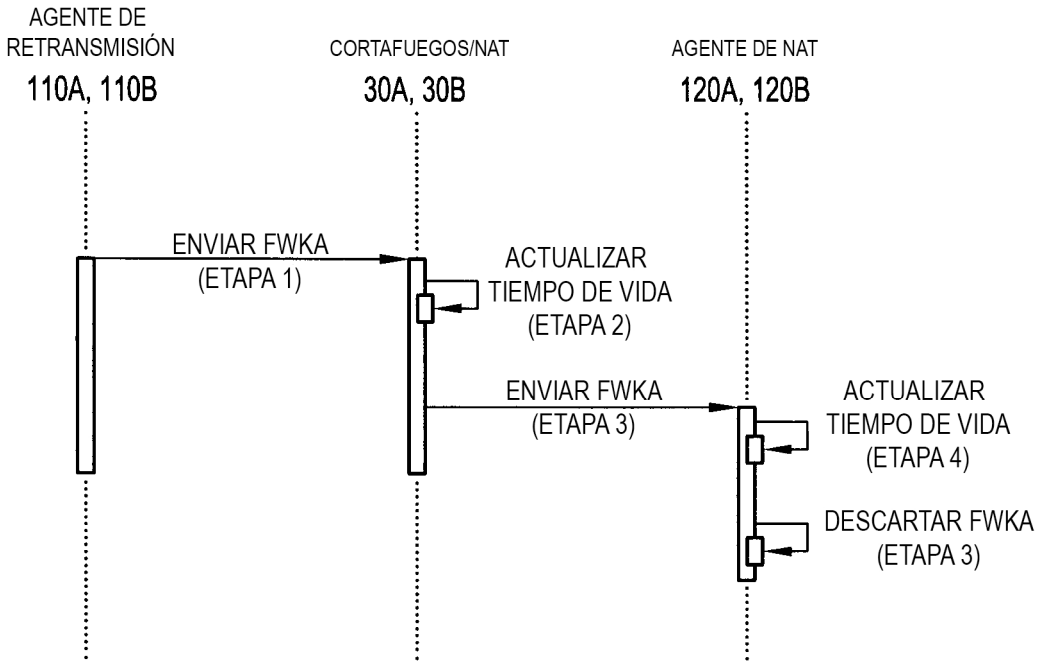
AGENTE DE RETRANSMISIÓN
110A, 110B
CORTAFUEGOS/NAT
30A, 30B
AGENTE DE NAT
120A, 120B
ENVIAR FWKA
(ETAPA 1)
ACTUALIZAR TIEMPO DE VIDA
(ETAPA 2)
ENVIAR FWKA
(ETAPA 3)
ACTUALIZAR TIEMPO DE VIDA
(ETAPA 4)
DESCARTAR FWKA
(ETAPA 3)

FIG. 7

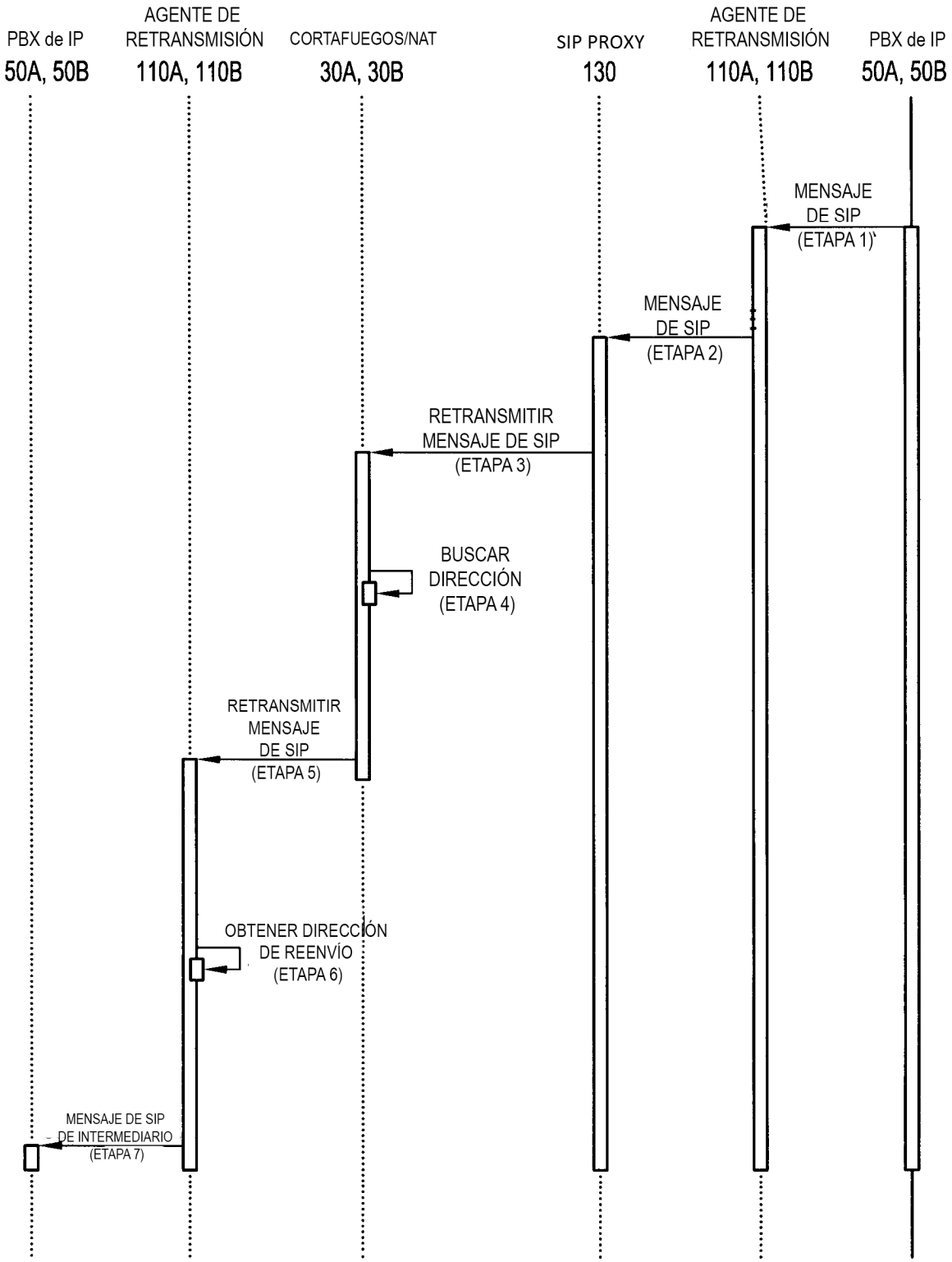
PBX de IP
50A, 50B
AGENTE DE RETRANSMISIÓN
110A, 110B
CORTAFUEGOS/NAT
30A, 30B
SIP PROXY
130
AGENTE DE RETRANSMISIÓN
110A, 110B
PBX de IP
50A, 50B
MENSAJE DE SIP (ETAPA 1)
MENSAJE DE SIP (ETAPA 2)
RETRANSMITIR MENSAJE DE SIP (ETAPA 3)
BUSCAR DIRECCIÓN (ETAPA 4)
RETRANSMITIR MENSAJE DE SIP (ETAPA 5)
OBTENER DIRECCIÓN DE REENVÍO (ETAPA 6)
MENSAJE DE SIP DE INTERMEDIARIO (ETAPA 7)

FIG. 8

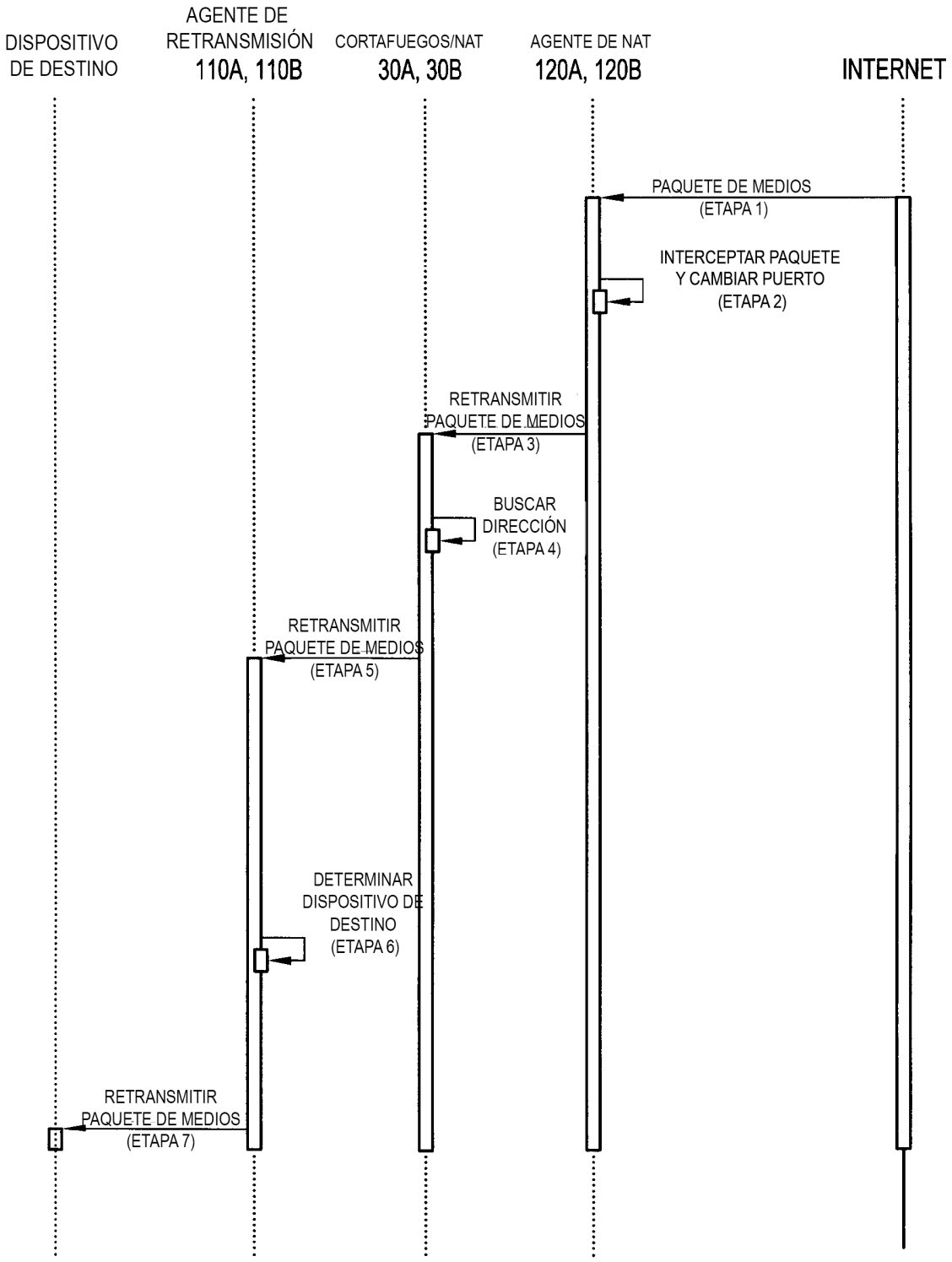
DISPOSITIVO DE DESTINO
AGENTE DE RETRANSMISIÓN 110A, 110B
CORTAFUEGOS/NAT 30A, 30B
AGENTE DE NAT 120A, 120B
INTERNET
PAQUETE DE MEDIOS (ETAPA 1)
INTERCEPTAR PAQUETE Y CAMBIAR PUERTO (ETAPA 2)
RETRANSMITIR PAQUETE DE MEDIOS (ETAPA 3)
BUSCAR DIRECCIÓN (ETAPA 4)
RETRANSMITIR PAQUETE DE MEDIOS (ETAPA 5)
DETERMINAR DISPOSITIVO DE DESTINO (ETAPA 6)
RETRANSMITIR PAQUETE DE MEDIOS (ETAPA 7)

FIG. 9

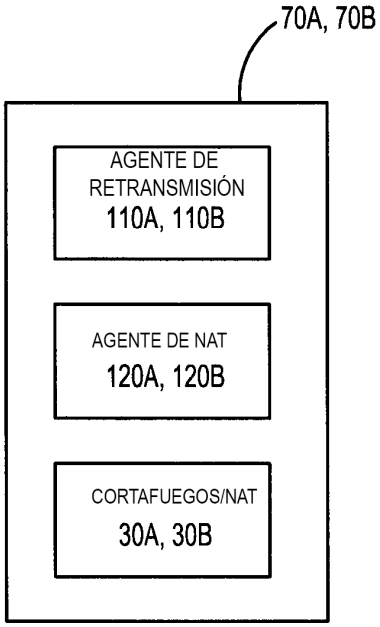
70A, 70B
AGENTE DE RETRANSMISIÓN
110A, 110B
AGENTE DE NAT
120A, 120B
CORTAFUEGOS/NAT
30A, 30B

FIG. 10

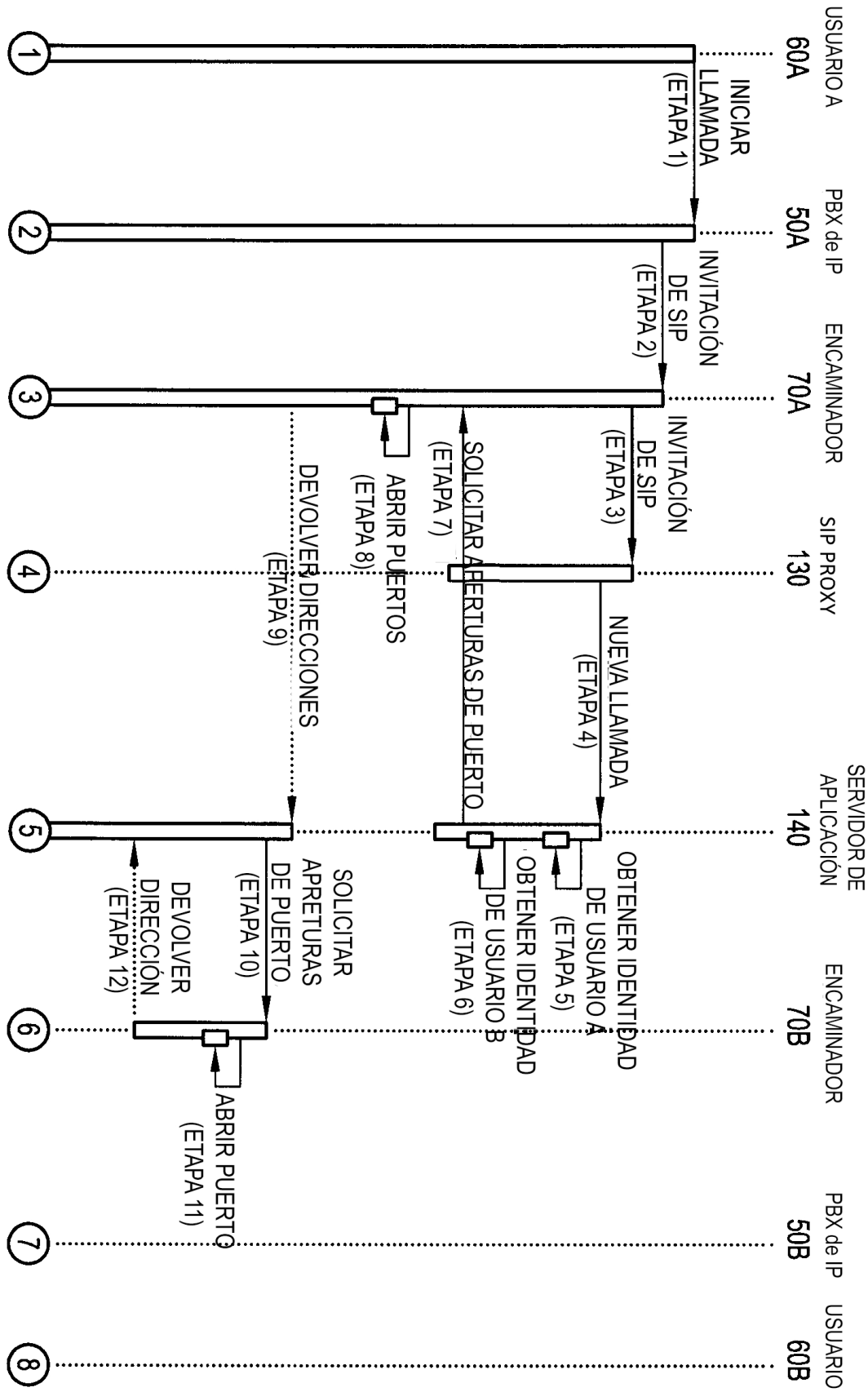
USUARIO A
60A
PBX de IP
50A
ENCAMINADOR
70A
SIP PROXY
130
SERVIDOR DE APLICACIÓN
140
ENCAMINADOR
70B
PBX de IP
50B
USUARIO B
60B
INICIAR LLAMADA (ETAPA 1)
INVITACIÓN DE SIP (ETAPA 2)
INVITACIÓN DE SIP (ETAPA 3)
NUEVA LLAMADA (ETAPA 4)
OBTENER IDENTIDAD DE USUARIO A (ETAPA 5)
OBTENER IDENTIDAD DE USUARIO B (ETAPA 6)
SOLICITAR APERTURAS DE PUERTO (ETAPA 7)
ABRIR PUERTOS (ETAPA 8)
DEVOLVER DIRECCIONES (ETAPA 9)
SOLICITAR APERTURAS DE PUERTO (ETAPA 10)
ABRIR PUERTO (ETAPA 11)
DEVOLVER DIRECCIÓN (ETAPA 12)
1
2
3
4
5
6
7
8

FIG. 11A

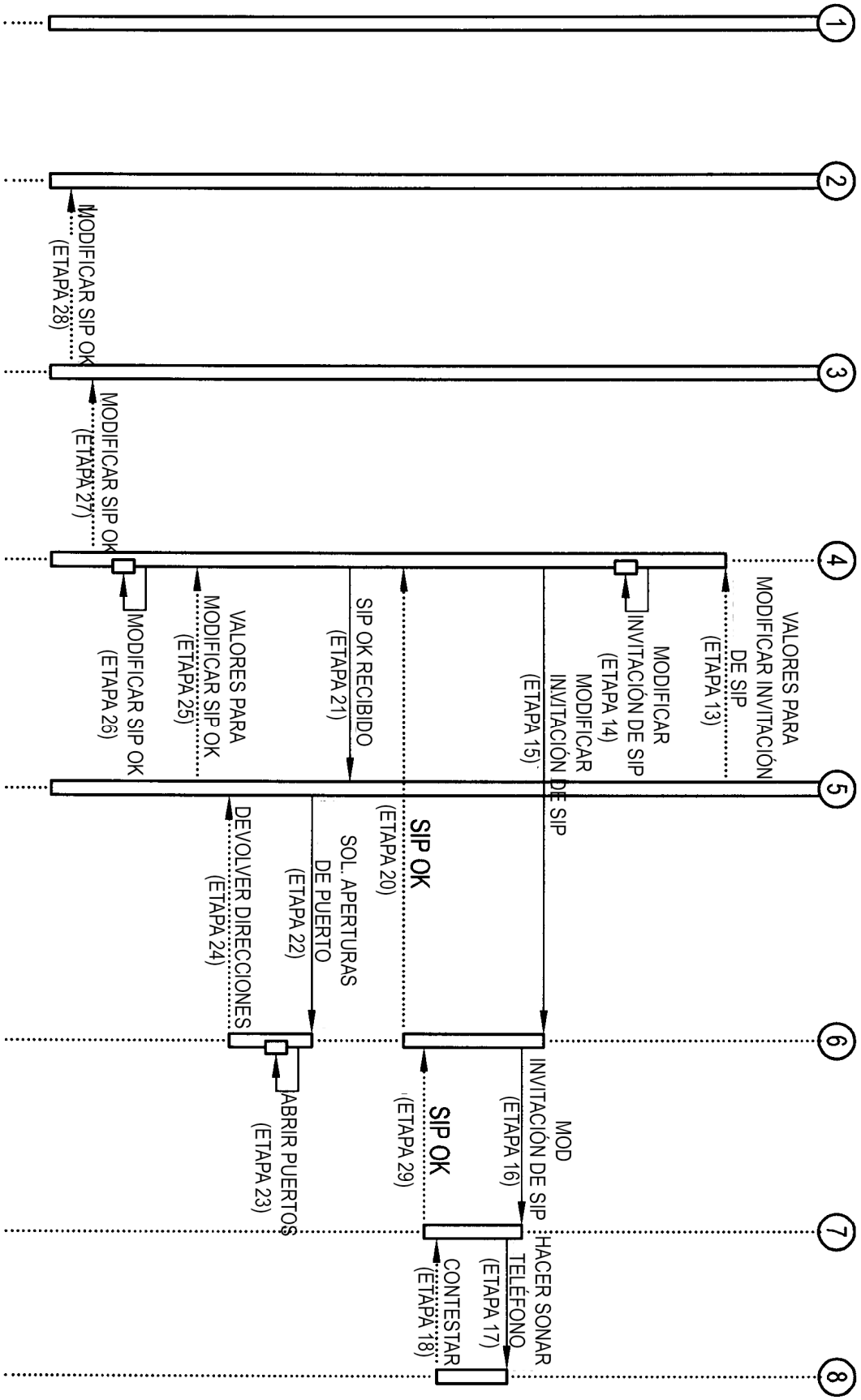
1
2
3
4
5
6
7
8
MODIFICAR SIP OK
(ETAPA 28)
MODIFICAR SIP OK
(ETAPA 27)
VALORES PARA
MODIFICAR INVITACIÓN
DE SIP
(ETAPA 13)
MODIFICAR
INVITACIÓN DE SIP
(ETAPA 14)
MODIFICAR
INVITACIÓN DE SIP
(ETAPA 15)
MODIFICAR SIP OK
(ETAPA 26)
VALORES PARA
MODIFICAR SIP OK
(ETAPA 25)
SIP OK RECIBIDO
(ETAPA 21)
SIP OK
(ETAPA 20)
DEVOLVER DIRECCIONES
(ETAPA 24)
SOL. APERTURAS
DE PUERTO
(ETAPA 22)
ABRIR PUERTOS
(ETAPA 23)
SIP OK
(ETAPA 29)
MOD
INVITACIÓN DE SIP
(ETAPA 16)
HACER SONAR
TELÉFONO
(ETAPA 17)
CONTESTAR
(ETAPA 18)

FIG. 11B

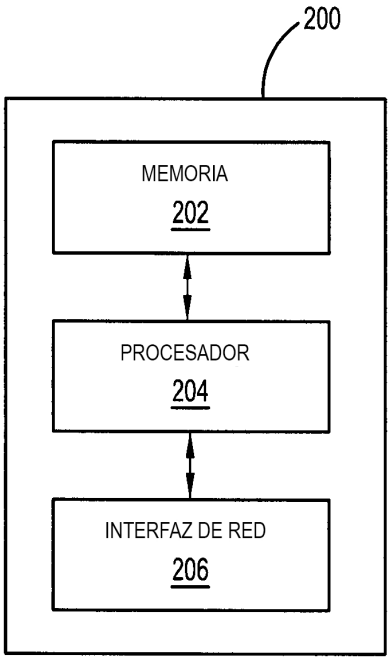

FIG. 12