(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 561 663**

(51) Int. CI.:

***H04W 12/06*** (2009.01)
***H04L 12/24*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.07.2011 E 11005641 (3)**

(97) Fecha y número de publicación de la concesión europea: **04.11.2015 EP 2547042**

(54) Título: **Método y sistema para gestionar dispositivos de red de distribuidores y fabricantes genéricos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**29.02.2016**

(73) Titular/es:

**TANAZA S.R.L. (100.0%)**
**Via C. De Cristoforis 13**
**20124 Milano, IT**

(72) Inventor/es:

**BERTANI, SEBASTIANO;**
**PIACENTE, CRISTIAN y**
**RINCON, RAY ANDREA**

(74) Agente/Representante:

**VALLEJO LÓPEZ, Juan Pedro**

## DESCRIPCIÓN

Método y sistema para gestionar dispositivos de red de distribuidores y fabricantes genéricos

La presente invención se refiere a un método y sistema para gestionar dispositivos de red de distribuidores y fabricantes genéricos.

El documento US 2004/0249931 desvela un sistema de gestión de red para monitorizar diversos atributos en dispositivos y elementos de red, que comprende un sistema de gestión de red (NMS), módulos de agente y dispositivos. A un usuario se le da la posibilidad de monitorizar nuevos atributos realizando un descubrimiento de los atributos de los dispositivos, seleccionado atributos específicos a partir de los atributos descubiertos e instanciar una instancia de monitorización que posibilita al usuario monitorizar los atributos seleccionados

El documento US 2005/0114397 y el documento WO 2004/093384 desvelan un método y sistema para gestión y configuración de agentes remotos, que proporciona una interfaz a un dispositivo que necesita gestionarse. En particular, estos documentos tienen por objeto posibilitar que un gestor descubra y gestione agentes remotos a través de cortafuegos, servidores intermediarios y/o VPN.

La difusión generalizada de puntos de acceso y otros dispositivos de red ha aumentado, en los últimos años, los costes de las compañías y de los individuos tienen que proporcionarse para gestionar, mantener y monitorizar esta multitud de dispositivos. Gestionar múltiples dispositivos de red tales como Puntos de Acceso Wi-Fi y CPE (Equipo de Instalación de Cliente) inalámbrico es una tarea que lleva mucho tiempo.

Las metodologías existentes para gestionar dispositivos de red, tales como puntos de acceso inalámbricos, pueden clasificarse en tres categorías principales: sistemas de gestión no centralizados, sistemas de hardware centralizado y sistemas de software remoto centralizado. Cada una de estas clases de tiene algunas desventajas como se describe a continuación.

Los sistemas de gestión no centralizados permiten a los administradores de red configurar y monitorizar cada dispositivo de red individualmente gracias a software, a menudo denominado firmware, instalado y que se ejecuta en el propio dispositivo. Diferentes distribuidores/fabricantes implementan protocolos propietarios en sus dispositivos que permiten al administrador de red acceder a ellos en diversas maneras, por ejemplo, interfaz web, interfaz CLI (Interfaz de Línea de Comandos), protocolo SSH (Intérprete Seguro (Secure SHell)).

Los sistemas de gestión no centralizados se adoptan normalmente en encaminadores, pasarelas y puntos de acceso de calidad de consumidor, para mercados sensibles al precio de gama baja. Las desventajas de este enfoque son la enorme cantidad de tiempo requerido para gestionar cada dispositivo en una manera uno a uno; la interfaz de usuario no homogénea proporcionada por cada distribuidor/fabricante; y la probabilidad aumentada de error humano ya que no puede adoptarse el algoritmo de comprobación de consistencia centralizado.

Los sistemas de hardware centralizado están diseñados normalmente para proporcionar herramientas de gestión sofisticadas adecuadas para mercados empresariales de gama alta. Estas soluciones requieren la instalación de un controlador de hardware, por ejemplo un servidor con una aplicación instalada, que permite al administrador de red configurar todos los dispositivos de red a través de una única interfaz, ahorrando tiempo y reduciendo costes de gestión. La desventaja de esta solución, normalmente preferida en fábricas grandes, aeropuertos, puertos, etc., es una inversión inicial o gasto de capital superior.

Los sistemas remotos basados en software centralizados permiten al administrador de red alcanzar y gestionar el dispositivo de red sin la necesidad de comprar un servidor o hardware especializado y de instalarlo físicamente. Ejemplos de estos sistemas se describen mediante el documento US 7.852.819, documento US 2008/0294759, documento US 2008/0285575 y documento US 2008/0304427.

Aunque estos sistemas son atractivos tanto desde el punto de vista de costes como de ahorro de tiempo, muestran también varias limitaciones y plantean desafíos como se describe a continuación.

Los dispositivos de red normalmente tienen que operar de acuerdo con procedimientos específicos para alcanzarse y gestionarse mediante el administrador de red, que implica por lo tanto el despliegue de firmware/software específico en todos los dispositivos controlables. Las soluciones desveladas mediante los documentos de patente anteriormente mencionados implican que los fabricantes de dispositivos de red de calidad empresarial desarrollen métodos y soluciones propietarios para configurar centralmente sus dispositivos de red. Esto significa que para poder usar un sistema remoto basado en software centralizado proporcionado mediante un fabricante específico, se solicita al usuario comprar e instalar en su red únicamente dispositivos de red producidos por dicho fabricante específico. Los dispositivos de red de distribuidores/fabricantes genéricos, tales como por ejemplo, dispositivos de red de calidad de consumidor de bajo coste, no pueden gestionarse.

Una desventaja adicional está relacionada con los procedimientos adoptados para proporcionar acceso remoto a los dispositivos de red que residen en una red privada de un usuario. En las soluciones desveladas mediante los documentos de patente anteriormente mencionados, la conexión entre la red anfitriona, es decir el controlador remoto, y los dispositivos de red se inicia y establece mediante cada único dispositivo de red de la red gestionada. Este aspecto representa una fuerte limitación en la escalabilidad del sistema.

Para superar las desventajas anteriormente mencionadas, el Solicitante tiene por objeto proporcionar un sistema remoto basado en software centralizado que permite gestionar dispositivos de red desde diversos distribuidores y fabricantes.

El documento US 2011/0087766 desvela una estructura de gestión de servicios y dispositivos unificada central operada para gestionar simultáneamente diversos tipos de recursos en beneficio de múltiples organizaciones.

Una desventaja de la solución desvelada mediante el documento US 2011/0087766 está relacionada con el hecho de que la conexión entre la instalación de gestión central y los dispositivos de red se inicia y establece mediante cada dispositivo de red único de la red gestionada. Este aspecto representa una fuerte limitación en la escalabilidad del sistema. Además, esta solución requiere aún el despliegue de firmware/software específico en todos los dispositivos de red controlables para posibilitarles hacer contacto inicial con la instalación central, después de que se han insertado en la red gestionada.

El Solicitante por lo tanto se enfrenta al problema técnico de proporcionar un sistema remoto basado en software centralizado mejorado que permita gestionar dispositivos de red desde distribuidores y fabricantes genéricos.

El Solicitante encontró que este problema puede resolverse mediante un método de acuerdo con la reivindicación 1.

En un segundo aspecto, la presente invención se refiere a un sistema de gestión remota de acuerdo con la reivindicación 11.

En un tercer aspecto, la presente invención se refiere a un programa informático de acuerdo con la reivindicación 12.

En un cuarto aspecto, la presente invención se refiere a un programa informático de acuerdo con la reivindicación 13.

En un aspecto adicional, la presente invención se refiere a un producto de programa informático que comprende medios de código de programa almacenados en un medio legible por ordenador para llevar a cabo las etapas con respecto al controlador remoto en el método de la invención.

En un aspecto adicional, la presente invención se refiere a un producto de programa informático que comprende medios de código de programa almacenados en un medio legible por ordenador para llevar a cabo las etapas con respecto al dispositivo de agente en el método de la invención.

En un aspecto adicional, la presente invención se refiere a un controlador remoto que comprende medios de hardware y/o software y/o firmware adaptados para llevar a cabo las etapas con respecto al controlador remoto en el método de la invención.

En un aspecto adicional, la presente invención se refiere a un dispositivo de agente que comprende medios de hardware y/o software y/o firmware adaptados para llevar a cabo las etapas con respecto al dispositivo de agente en el método de la invención.

Las reivindicaciones dependientes hacen referencia a realizaciones particularmente ventajosas de la invención.

En la presente descripción y reivindicaciones, los términos:

- “red” se usa para indicar cualquier red de área extensa o local, cableada, inalámbrica, cableada/inalámbrica híbrida;

- “dispositivo de red” se usa para indicar cualquier dispositivo de una red tal como un encaminador, una pasarela, un punto de acceso, un servidor, un dispositivo de cliente (tal como un PC, tableta, portátil, teléfono móvil y similares);

- “nodo” se usa para indicar un dispositivo de red a gestionar mediante un controlador remoto. Ejemplos de nodos son encaminadores, puntos de acceso, puntos de acceso, cortafuegos y discos duros en red;

- “conexión de túnel” se usa para indicar una conexión establecida entre dispositivos de red que encapsula un protocolo de red, dicho “protocolo de cabida útil”, dentro de los mensajes de otro protocolo de red, dicho “protocolo de entrega”. Este mecanismo permite que se entregue el protocolo de cabida útil incluso si no está

permitido explícitamente por obstáculos de red tales como cortafuegos, traductores NAT, pasarelas, intermediarios, etc..., que en su lugar, permiten que se entregue el protocolo de entrega;

- "protocolo de tunelización" se usa para indicar un protocolo específico adaptado para implementar una conexión de túnel. Cada protocolo de tunelización puede entregarse a través de un subconjunto específico de obstáculos de red.

Las características y ventajas adicionales de la presente invención se harán más evidentes a partir de la siguiente descripción detallada de algunas realizaciones preferidas de la misma, realizadas como un ejemplo y no para fines de limitación con referencia a los dibujos adjuntos. En tales dibujos,

- la figura 1 muestra esquemáticamente un sistema de acuerdo con una realización de la invención;

- la figura 2 muestra esquemáticamente un sistema de acuerdo con otra realización de la invención;

- la figura 3 muestra esquemáticamente un controlador remoto de acuerdo con una realización de la invención;

- las figuras 4A y 4B muestran esquemáticamente una base de datos de controlador remoto de acuerdo con dos realizaciones de la invención;

- las figuras 5A y 5B muestran esquemáticamente la estructura de una sección de la base de datos de controlador remoto de acuerdo con dos realizaciones de la invención;

- la figura 6 muestra esquemáticamente un dispositivo de agente de acuerdo con una realización de la invención;

- la figura 7 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de tunelización de acuerdo con una realización de la invención;

- la figura 8 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de descubrimiento de acuerdo con una primera realización de la invención;

- la figura 9 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de descubrimiento de acuerdo con una segunda realización de la invención;

- la figura 10 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de descubrimiento de acuerdo con una tercera realización de la invención;

- la figura 11 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de descubrimiento de acuerdo con una cuarta realización de la invención;

- la figura 12 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de evasión de conflictos de IP de acuerdo con una realización de la invención;

- la figura 13 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de evasión de conflictos de subred de acuerdo con una realización de la invención;

- la figura 14 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de identificación de acuerdo con una primera realización de la invención;

- la figura 15 muestra un diagrama de flujo de un algoritmo para implementar un procedimiento de identificación de acuerdo con una segunda realización de la invención.

La Figura 1 muestra un sistema de gestión de dispositivo de red 10 de acuerdo con una realización de la invención, que comprende un controlador remoto 1 (en la presente descripción y dibujos denominado también como "controlador multi-distribuidor" o MVC), una red de área extensa (WAN) 2 y una red de área local (LAN) 100. En la realización ejemplar, el controlador remoto 1 está localizado en la WAN 2, la WAN 2 comprende internet, y la LAN 100 comprende una pluralidad de dispositivos de red 110, 120 y 130.

En una realización preferida de la invención, la LAN 100 es una LAN Ethernet/IP (Protocolo de Internet) LAN. Es decir, la LAN 100 puede tener cualquier capa física, y tiene una capa 2 de Ethernet (o capa de enlace de datos) y una capa 3 de IP (o capa de red). Preferentemente, la LAN 100 soporta protocolos de traducción para resolución de direcciones de capa 3 (por ejemplo direcciones de IP) en direcciones de capa 2 (por ejemplo Control de Acceso al Medio o direcciones de MAC) y vice-versa. Ejemplos de estos protocolos son respectivamente ARP (Protocolo de Resolución de Dirección) y RARP (Protocolo de Resolución de Dirección Inverso) bien conocidos en la técnica y especificados, por ejemplo, mediante el documento RFC 826 y documento RFC 903.

Los dispositivos de red pueden ser encaminadores, puntos de acceso, pasarelas, servidores locales, dispositivos de cliente (tales como PC, tableta, portátil, teléfono móvil,...) cableados o inalámbricos y similares.

Los dispositivos de red a gestionar mediante el controlador remoto 1 se denominan en lo sucesivo como nodos. Los nodos pueden ser cualquier dispositivo de red que pueda requerir configurarse o gestionarse tal como, por ejemplo, puntos de acceso (AP), encaminadores, pasarelas, cortafuegos, discos duros en red.

Como se explica en más detalle a continuación, gracias a la invención, los nodos a gestionar mediante el controlador remoto 1 pueden ser de cualquier distribuidor/fabricante y pueden identificarse mediante ninguna clase específica o intervalo de direcciones (MAC).

En la figura 1, la LAN 100 comprende una pasarela (GW) 130 para conexión a Internet 2, un dispositivo de agente 120 y cuatro nodos 110 a gestionar.

El dispositivo de agente 120 es un componente intermedio del sistema 10 que permite al controlador remoto 1 comunicar con cualquier nodo de la LAN gestionada 100.

En particular, el dispositivo de agente puede ser cualquier dispositivo de red de la LAN 100 en el que se despliega una utilidad de agente (es decir programa informático), que está adaptada para llevar a cabo las etapas del método de gestión de la invención relacionadas con el dispositivo de agente. Ventajosamente, el dispositivo de red en el que se despliega la utilidad de agente es un servidor local de la LAN, que es un dispositivo siempre en ejecución. Sin embargo, puede ser también un dispositivo de cliente o un nodo a gestionar, como se muestra ejemplarmente en la realización de la figura 2.

La utilidad de agente es un software y/o firmware que puede instalarse en un servidor local de la LAN 100, pero puede representarse también mediante un software en ejecución temporal en un dispositivo de cliente dentro la LAN 100, por ejemplo un activex o una extensión de explorador que está activa únicamente cuando el usuario activa una interfaz adecuada del dispositivo cliente, tal como un sitio web en su portátil, PC o dispositivo similar.

El dispositivo de agente 120 puede comprender una o más interfaces, cubriendo cada una una subred de nodos 110 de la LAN 100. Cada interfaz se identifica ventajosamente mediante un identificador de interfaz específico (por ejemplo: interfaz 1, interfaz 2,...interfaz n) y cada subred se identifica mediante un identificador que representa una parte de la dirección de IP (normalmente la porción de cabecera de la dirección de IP) que debería compartirse entre todos los nodos 110 que pertenecen a la subred. Por ejemplo, considerando una dirección de IP de 32 bits compuesta de 4 secciones A.B.C.D, el identificador de subred puede representar la sección o secciones iniciales A, A.B, o A.B.C. o una sección intermedia (por ejemplo B o B.C).

Incluso si en la realización de la figura 1 la LAN 100 comprende un único dispositivo de agente 120, cada LAN puede comprender entonces más de un dispositivo de agente, como se muestra en la realización de la figura 2. Sin embargo, de acuerdo con la invención, la LAN 100 tiene ventajosamente un número de dispositivos de agente que es inferior al número de nodos a gestionar.

El MVC 1 es el elemento de red a través del cual el usuario o usuarios (por ejemplo el administrador o administradores de red) pueden alcanzar todos los nodos que pueden configurarse, gestionarse o monitorizarse. En la realización de la figura 1, el MVC 1 es un servidor centralizado disponible en internet. Sin embargo, el controlador remoto puede localizarse también en una nube pública, en una intranet, en una nube privada, o incluso en la LAN para escalabilidad o razones de seguridad.

La expresión controlador remoto se usa para indicar un anfitrión remoto centralizado o una utilidad de software/firmware (es decir programa informático) desplegado en un anfitrión remoto centralizado.

Por ejemplo, en la realización de la figura 2, el sistema comprende cinco LAN 100, 200, 300, 400, 500, internet 2 y tres MVC 1, 1’ y 1”. El MVC 1 es un controlador multi-distribuidor disponible como un servicio en la nube público, el MVC 1’ está localizado en una nube privada, es decir una red des-localizada controlada mediante una compañía, y el MVC 1” está localizado dentro de la LAN 500 del cliente, para cumplir políticas de seguridad de red específicas especificadas por el administrador de red o por la compañía.

En la realización de la figura 2, la LAN 100 está conectada a internet a través de la pasarela 130, comprende un único dispositivo de agente 120 y una pluralidad de nodos 110 y dispositivos de cliente 140.

La LAN 200 está conectada a internet a través de la pasarela 230 y comprende una pluralidad de nodos 210 y dispositivos de cliente 240. Para aumentar la disponibilidad del sistema de gestión, la LAN 200 comprende dos dispositivos de agente 220-1 y 220-2 que pueden operarse de manera alternativa (mecanismo de respaldo).

La LAN 300 representa una red organizada jerárquicamente que comprende una sub-red 300’.

La LAN 300 está conectada a internet a través de la pasarela 330 mientras que la sub-red 300' está conectada jerárquicamente a internet a través de la pasarela 330' y 330. La LAN 300 comprende adicionalmente un primer dispositivo de agente 320-1, un segundo dispositivo de agente 320-2, un tercer dispositivo de agente 320-3, una pluralidad de nodos 310, 310' y dispositivos de cliente 340, 340'. El segundo dispositivo de agente 320-2, la pasarela 330', los puntos de acceso 310' y los dispositivos de cliente 340' son parte de la subred 300'. El tercer dispositivo de agente 320-3 se despliega dentro de un dispositivo de cliente 340. Esto puede implementarse en diversas maneras, tal como una mini aplicación de java, un active-x, una extensión de explorador, una aplicación instalada en el cliente, etc. El aspecto común del despliegue-en-cliente de la utilidad de agente es el hecho de que cuando el cliente está desconectado, si no está disponible otro dispositivo de agente para la red específica, entonces esa red no podría ser gestionable; este no es el caso de la red 300, ya que el primer dispositivo de agente 320-1 sustituiría al tercer dispositivo de agente 320-3 (mecanismo de respaldo).

La LAN 400 está conectada a internet a través de la pasarela 430, comprende dos dispositivos de agente 420-1, 420-2 y una pluralidad de nodos 410 y dispositivos de cliente 440. Los dos dispositivos de agente 420-1, 420-2 se implementan en dos nodos 410 (es decir, la utilidad de agente se despliega en dos nodos 410). Los dos dispositivos de agente 420-1, 420-2 permiten, individualmente, operar en todos los nodos 410 de la LAN 400.

La LAN 500 está conectada a internet a través de la pasarela 530, comprende un único dispositivo de agente 520 y una pluralidad de nodos 510 y dispositivos de cliente 540.

Los dispositivos de agente están configurados para conectarse a un MVC específico, que puede estar disponible en internet, en una nube privada o localmente. Por ejemplo, en la figura 2, los dispositivos de agente 120, 220-1, 220-2, y 320-1 están configurados para conectarse al MVC 1 localizado en un servicio de nube pública; los dispositivos de agente 320-2, 420-1 y 420-2 están configurados para conectarse al MVC 1' localizado en un servicio de nube privada, y el dispositivo de agente 520 está configurado para conectarse al MVC 1", desplegado localmente.

Cada controlador remoto y dispositivo de agente en el sistema 10 y en la o las LAN (a continuación denominados únicamente con los números de referencia 1, 120, y 100, respectivamente) comprende módulos de hardware y/o software y/o firmware adaptados para implementar las etapas correspondientes del método de gestión de la invención.

Como se explica adicionalmente en lo sucesivo, gracias a la invención, los dispositivos de red distintos del dispositivo de agente y del controlador remoto no necesitan que se realice adaptación específica para implementar el método de gestión. En particular, una innovación crucial de la invención reivindicada es el hecho de que no se requiere desplegar ningún software específico en los nodos a gestionar, ni asumir ningún procedimiento o comportamiento específico, para gestionarlos.

De acuerdo con el método de gestión de la invención:

- el dispositivo de agente hace un contacto inicial con el controlador remoto 1 para autenticarse y establecer una conexión con el controlador remoto 1;

- después de que se establece la conexión, el controlador remoto 1 ejecuta un procedimiento de descubrimiento por la intermediación del dispositivo de agente 120 para descubrir los nodos 110 de la LAN 100 a gestionar;

- después de ejecutar el procedimiento de descubrimiento, el controlador remoto 1 identifica los nodos descubiertos 110 por la intermediación del dispositivo de agente 120;

- el controlador remoto 1 gestiona los nodos descubiertos e identificados 110 por la intermediación del dispositivo de agente 120, usando procedimientos de gestión específicos para los nodos identificados 110.

Para implementar el método de gestión de la invención, el controlador remoto 1 comprende ventajosamente tres sub-componentes lógicos, informados en la figura 3: una base de datos 14; un extremo trasero 12; y un extremo frontal 16.

Un usuario, en lo sucesivo denominado como un administrador de red, puede interactuar con el controlador remoto 1 para acceder, configurar, controlar y monitorizar los nodos 110 a través de al menos una interfaz de usuario UI 18. Las interfaces de usuario 18 pueden ser interfaces de línea de comandos, aplicaciones de escritorio, aplicaciones web, aplicaciones de dispositivos móviles tales como aplicaciones de iPad, iPhone o Android, herramientas y similares. La al menos una interfaz de usuario UI 18 está adaptada para intercambiar información con el extremo frontal 16.

El extremo frontal 16 permite, a través de la interfaz de usuario UI 18, que el administrador de red elija qué nodos 110 acceder, configurar, controlar y monitorizar.

La base de datos 14 incluye ventajosamente una lista de nodos 110 a gestionar. Esta lista puede crearse mediante el administrador de red o puede generarse automáticamente mediante el controlador remoto 1 y, opcionalmente, confirmarse por el administrador de red. La base de datos 14 incluye también ventajosamente un conjunto de protocolos y procedimientos requeridos para acceder, configurar, controlar y monitorizar nodos fabricados por diferentes fabricantes/distribuidores, cada uno de ellos caracterizados por parámetros caracterizadores de dispositivo específicos, tales como, por ejemplo, modelo, distribuidor, fabricante, versión de software, versión de hardware, versión de firmware, número de serie y/o dirección de MAC.

El extremo trasero 12 es el sub-componente del controlador remoto 1 que permite establecer la comunicación entre el controlador remoto 1 y el dispositivo de agente 120.

La base de datos 12, el extremo trasero 14 y el extremo frontal 16 pueden desplegarse físicamente en un mismo servidor, como se informa en la Figura 3, o en diferentes servidores o servidores o nubes virtuales, privados o públicos.

La Figura 4A muestra una realización de la estructura para la base de datos 14 que comprende: una primera sección 900 que contiene una lista de nodos, identificados, por ejemplo, mediante direcciones de IP (Protocolo de Internet) y/o de MAC (Control de Acceso al Medio); una segunda sección 910 en la que los nodos de la lista (identificados mediante sus direcciones de IP y/o de MAC (Control de Acceso al Medio)) están asociados a parámetros caracterizadores de dispositivo específicos tales como modelo, distribuidor, fabricante, versión de software, versión de hardware, versión de firmware y/o número de serie; una tercera sección 920 en la que los nodos de la lista están asociados a parámetros de configuración específicos que pueden especificarse mediante el administrador de red; y una cuarta sección 930 que comprende una pluralidad de procedimientos de gestión, cada uno asociado a parámetros caracterizadores de dispositivo específicos tales como, por ejemplo, modelo, distribuidor, fabricante, versión de software, versión de hardware, versión de firmware y/o número de serie.

La estructura de la figura 4B es similar a la figura 4A excepto por el hecho de que comprende adicionalmente una quinta sección 911 que comprende una lista de secuencias de procedimientos de conexión, como se explica adicionalmente en detalle en el presente documento más adelante, cuando se trata con el procedimiento de identificación de nodos de la figura 15.

Como se muestra en la figura 5A, en la primera sección 900 los nodos pueden clasificarse en “nodos disponibles” 901, “nodos no alcanzables” 902, y “nodos descubiertos” 903.

Como se muestra en la figura 5B, en la cuarta sección 930 los procedimientos de gestión pueden clasificarse en procedimientos de conexión 931, procedimientos de configuración/control 932 y procedimientos de monitorización 933. Los procedimientos de gestión pueden implementarse de acuerdo con protocolos y/o mecanismos soportados mediante interfaces propietarias de los nodos 110 a gestionar. Ejemplos de tales protocolos y mecanismos bien conocidos en la técnica son los siguientes: CLI (Interfaz de Línea de Comandos), SSH (Intérprete Seguro, como por ejemplo definido mediante el documento RFC4251), protocolo Telnet, HTTP (Protocolo de Transferencia de Híper Texto, como por ejemplo definido mediante el documento RFC2616), HTTPS (Protocolo de Transferencia de Híper Texto sobre Capa de Conector (Socket) Segura, como por ejemplo definido mediante el documento RFC2818), SMTP (Protocolo de Gestión de Red Simple, como por ejemplo definido mediante el documento RFC1157), protocolo OPC (Conectividad Abierta como se describe por ejemplo en el sitio web opcfoundation.org), arquitectura SCADA (Control de Supervisión y Adquisición de Datos), mecanismo para descargar fichero o ficheros de configuración desde un nodo y cargarlos en el nuevo fichero o ficheros de configuración de nodo con parámetros modificados, tales como FTP (Protocolo de Transferencia de Ficheros, como por ejemplo definido mediante el documento RFC959), TFTP (Protocolo de Transferencia de Ficheros Trivial, como por ejemplo definido mediante el documento RFC1350), SCP (Protocolo de Copia Segura); mecanismo que simula la navegación de un usuario virtual a través de la interfaz basada en web de un nodo, emulando comandos de navegación, tales como peticiones basadas en HTTP, peticiones basadas en HTTPS, interacciones AJAX (JavaScript Asíncrono y XML).

Para implementar el método de gestión de la invención, el dispositivo de agente 120 comprende ventajosamente una interfaz de usuario 129, una sección de configuración de agente 121, una sección de conexión de tunelización 124, una sección de operación 125, una sección de conexión LAN 126, una sección de mecanismo de tunelización 127, una sección de descubrimiento de agente de par 128, como se muestra en la figura 6.

La sección de configuración de agente 121, a su vez, comprende una sección de configuración de tunelización 122 y una sección de restricciones de seguridad 123.

La sección de configuración de tunelización 122 comprende ventajosamente parámetros requeridos mediante mecanismos de tunelización específicos (tales como, por ejemplo, direcciones de MVC, parámetros de autenticación de intermediario, etc.) o exclusión administrativa de mecanismos de tunelización específicos (por ejemplo por razones de seguridad).

La sección de restricciones de seguridad 123 permite al usuario denegar el acceso a nodos específicos 110 y ser compatible con políticas de seguridad estrictas. Si estas restricciones se especifican, tanto el dispositivo de agente 120 como el controlador remoto 1 no podrán alcanzar los nodos restringidos 110.

La sección de conexión de túnel 124 está adaptada, en cooperación con la sección de mecanismo de tunelización 127, para establecer una conexión de túnel con un controlador remoto especificado 1 tomando las acciones apropiadas para superar diversos obstáculos de red que pueden evitar que el dispositivo de agente 120 se conecte satisfactoriamente al controlador remoto 1, como se explica en más detalle en el presente documento más adelante con referencia a la figura 7. Dichos obstáculos pueden incluir traductores NAT, cortafuegos, intermediarios, modeladores de tráfico y similares.

La sección de operación 125 está adaptada para posibilitar la ejecución de operaciones, tales como procedimientos de gestión (que pueden clasificarse en procedimientos de conexión 931, procedimientos de configuración/control 932 y procedimientos de monitorización 933) solicitados mediante el controlador remoto 1 para un nodo específico 110, y etapas de procedimiento de tunelización, procedimiento de descubrimiento, procedimiento de identificación, procedimiento de evasión de conflictos de IP, procedimiento de evasión de conflictos de subred, descritos en detalle en el presente documento más adelante.

La sección de conexión de LAN 126 está adaptada para establecer conexiones de LAN con los nodos 110 de acuerdo con técnicas conocidas en la técnica, tales como por ejemplo Ethernet (IEEE 802.3), WiFi (IEEE 802.11), Fibra Óptica u otras normas de red.

La sección de mecanismo de tunelización 127 está adaptada para ejecutar un procedimiento de tunelización, como se explica en más detalle en el presente documento más adelante con referencia a la figura 7.

La sección de descubrimiento de agente de par 128 está adaptada para implementar un procedimiento de descubrimiento de par para descubrir cualquier otro dispositivo de agente que pueda estar presente en la LAN. Este procedimiento se describe en más detalle a continuación, con referencia a la figura 7.

La interfaz de usuario 129 posibilita al usuario (por ejemplo, el administrador de red) interactuar directamente con el dispositivo de agente 120.

Una ventaja de la invención es que no necesita mantenerse una conexión de túnel entre el controlador remoto 1 y cada nodo individual 110 de la LAN 100, ya que la conexión de túnel se establece únicamente con el único dispositivo de agente 120 (o con un número de dispositivos de agente inferior al número total de nodos 110 de la LAN).

Este aspecto es ventajoso, en comparación con otras soluciones, por las siguientes razones:

- permite reducir los recursos requeridos en el controlador remoto 1, ya que el número de conexiones se disminuye en un factor K, igual al número medio de nodos 110 para el dispositivo de agente 120;

- permite reducir los recursos requeridos en los nodos gestionados 110, ya que no se requiere ninguna conexión permanente entre los nodos 110 y el controlador remoto 1;

- reduce la ocupación de ancho de banda, ya que el dispositivo de agente 120 puede adoptar diversas técnicas de compresión y agregación de tráfico bien conocidas que permiten una reducción del tráfico tanto en término de número de paquetes por segundo como de bytes por segundo. El número de paquetes por segundo se reduce de K*fs, en la solución no basada en dispositivo de agente, (donde K es el número de nodos medio 110 por dispositivo de agente 120 y fs es la frecuencia con la que se envía una información) a 1*fs en la solución de la invención, reduciendo por lo tanto el número de paquetes de un factor K y ahorrando potencia de procesamiento en cada nodo 110. Por otra parte, el tráfico expresado en términos de bytes por segundo se reduce de K*fs*D (donde D es el tamaño de paquete medio en soluciones no basadas en dispositivo de agente) o K*fs*D' (donde D'<D es el tamaño de paquete medio en soluciones de no dispositivo de agente que implementan una compresión local en los nodos 110) a 1*fs*(K*D"), donde K*D" es el tamaño medio del paquete que se envía mediante el dispositivo de agente 120 e incluye toda la información de los K nodos 110. Este paquete tiene un tamaño medio K*D"<K*D'<K*D gracias a la compresión proporcionada mediante técnicas bien conocidas que no pueden adaptarse en soluciones no basadas en dispositivo de agente. De hecho, estas técnicas aprovechan la información mutua, o correlación, entre paquetes para alcanzar relaciones de compresión superiores.

Para conectarse al controlador remoto 1, el dispositivo de agente 120 establece una conexión de túnel usando diversas técnicas para superar los obstáculos de red anteriormente mencionados que incluyen, pero sin limitación, traductores NAT, bloqueos de UDP, cortafuegos, pasarelas, modeladores de tráfico, intermediarios de http, intermediarios de https, intermediarios de conectores y así sucesivamente.

Las técnicas de tunelización, por ejemplo túnel de UDP, conocidas en la técnica pueden pasar únicamente un

subconjunto de dichos obstáculos de red (por ejemplo traductores NAT). Esto requiere que el administrador de red modifique las políticas de seguridad de la LAN para garantizar la comunicación apropiada con el controlador remoto 1. Desafortunadamente, especialmente en grandes empresas y corporaciones, no siempre es posible modificar tales políticas.

El procedimiento de tunelización propuesto mediante la invención tiene por objeto garantizar una conexión de túnel independientemente de cualquier política de seguridad configurada en la LAN 100, sin requerir ningún cambio de tales políticas de seguridad.

Esto se obtiene gracias a un procedimiento en el que el dispositivo de agente 120 intenta en secuencia una pluralidad de protocolos de tunelización para establecer una conexión de túnel con el controlador remoto 1, hasta que se establece satisfactoriamente una conexión de túnel.

La pluralidad de protocolos de tunelización intentados mediante el dispositivo de agente 120 pueden ser los siguientes protocolos conocidos en la técnica: tunelización de ip-sobre-ip; tunelización de ip-sobre-udp; tunelización de ip-sobre-tcp; tunelización de ip-sobre-http; tunelización de ip-sobre-http a través de intermediario (http, https, conectores, etc.); tunelización de http a través de intermediario y modelador de tráfico.

La Figura 7 muestra una realización ejemplar del algoritmo para implementar el procedimiento de tunelización de acuerdo con la invención.

En el bloque 701, el dispositivo de agente 120 establece todos los protocolos de tunelización disponibles como “no intentados”. Los protocolos no configurados, es decir los que requieren que se especifique algún parámetro de configuración mediante el administrador de red (por ejemplo dirección de intermediario en caso de tunelización de http a través de intermediario) se descartan. Además, el administrador de red podría decidir excluir protocolos específicos de la lista, para ser compatible con reglas o políticas de seguridad predeterminadas. En este caso, los protocolos excluidos no se intentarán.

En el bloque 702, el dispositivo de agente 120 selecciona el protocolo que tiene el coste inferior entre los etiquetados como “no intentados”. Ya que cada protocolo puede pasar diferentes tipos de obstáculos de red y tiene un coste específico en términos de recursos requeridos tanto en el dispositivo de agente como en el servidor o plataforma de nube donde se ejecuta el controlador remoto 1, el coste puede representar los recursos requeridos en el dispositivo de agente 120 y/o controlador remoto 1. Los recursos requeridos pueden incluir potencia computacional, ancho de banda de red, consumo de potencia, uso de memoria o cualquier otro aspecto que pueda ser pertinente para la red específica.

El coste asociado a cada protocolo puede asignarse de diversas maneras. Por ejemplo, puede ser un número entero arbitrario (1: paquetes de ip, 10: túnel de udp, 100: túnel de tcp, 1000: túnel de http,...).

En el bloque 703 el dispositivo de agente intenta establecer una conexión de túnel con el controlador remoto 1 usando el protocolo de tunelización seleccionado.

En el bloque 704, el dispositivo de agente 120 comprueba si se establece la conexión.

En caso positivo, en el bloque 705 el dispositivo de agente 120 permanece en una condición en reserva, esperando instrucciones desde el controlador remoto 1 o los nodos 110.

En caso negativo, en el bloque 706 el dispositivo de agente 120 descarta el protocolo intentado y vuelve al bloque 702 para intentar otro protocolo de tunelización -aún no intentado- a un coste superior. En el escenario del peor caso, el protocolo seleccionado será el de con el coste más alto (esto suponiendo que hay al menos un protocolo que posibilita que el dispositivo de agente 120 acceda a la red externa (por ejemplo internet).

En una realización preferida, el algoritmo comprende también los bloques 707 y 708. En el bloque 707, una vez conectado, el dispositivo de agente 120 comprueba si hay algún otro dispositivo de agente en la misma LAN 100. En caso negativo, el algoritmo finaliza. En caso positivo, en el bloque 708 el dispositivo de agente 120 elige actuar como dispositivo de agente activo o agente de respaldo basándose en una comparación de coste: el dispositivo de agente con el coste más bajo actúa como activo mientras que el otro actúa como dispositivo de agente de respaldo. Un ejemplo de métrica para comparación de coste es la disponibilidad de tiempo del dispositivo de agente: esta métrica permitiría al sistema usar dispositivos de agente que están residentes en un servidor local y considerar activex de cliente o agentes similares como respaldo.

Dos estrategias ejemplares para permitir al dispositivo de agente 120 descubrir la existencia de dispositivos de agente concurrentes en la misma LAN son las siguientes: centralizada y basada en pares. En la estrategia centralizada, el controlador remoto 1 compara la lista de nodos 110, por ejemplo la dirección de MAC, asociada a cada dispositivo de agente 120; si dos dispositivos de agente están asociados a la misma lista de nodos 110, se consideran concurrentes y el controlador remoto 1 decide qué dispositivo de agente 120 debe actuar como respaldo.

En la estrategia basada en pares cada dispositivo de agente 120 envía paquetes de difusión para establecer una conexión a otros dispositivos de agente de pares 120 en la misma LAN 100; estos paquetes contienen información acerca de la conectividad real al controlador remoto 1 y coste; cada dispositivo de agente 120 puede decidir individualmente actuar como agente de respaldo o activo para la LAN 100. Ambas de estas soluciones tienen puntos fuertes y debilidades: el enfoque centralizado simplifica la estructura del dispositivo de agente y no hace suposición sobre conectividad intra-LAN de agente pero requiere recursos superiores en el controlador remoto 1; el enfoque basado en pares reduce los recursos usados mediante el controlador remoto 1, pero requiere una complejidad superior en los dispositivos de agente 120.

Como se ha indicado anteriormente, después de que el dispositivo de agente 120 establece una conexión de túnel con el controlador remoto 1, el controlador remoto 1 ejecuta un procedimiento de descubrimiento por la intermediación del dispositivo de agente 120 para descubrir los nodos 110 de la LAN 100.

El procedimiento de descubrimiento incluye intentar establecer una conexión con los nodos 110, por la intermediación del dispositivo de agente 120, usando la dirección de IP y/o dirección de MAC predeterminadas, o usando un procedimiento de exploración automático (no requiriendo ninguna información desde el administrador de red) que explora una multitud predeterminada de direcciones de IP para intentar establecer una conexión con los nodos 110.

La Figura 8 muestra una primera realización de un procedimiento de descubrimiento, haciendo uso de tanto direcciones de IP como de MAC.

En el bloque 801 el administrador de red especifica al controlador remoto 1 las direcciones de IP y de MAC de un nodo específico 110 a descubrir.

En esta realización y en las otras realizaciones de las figuras 9, 10, 11, 14 y 15 en el presente documento descritas más adelante, cada vez que haya más de un dispositivo de agente 120, el administrador de red puede seleccionar cuál es el dispositivo de agente preferido a usar o puede dejar esta elección al controlador remoto 1. En el último caso el controlador remoto 1 puede seleccionar, por ejemplo, el dispositivo de agente que minimiza o maximiza alguna métrica relacionada con el nodo 110 y el propio el dispositivo de agente 120 (por ejemplo maximizar disponibilidad de la conexión entre el dispositivo de agente 120 y el nodo 110, minimizar la diferencia entre la dirección de IP de interfaz de dispositivo de agente y la dirección de IP del nodo, minimizar el tiempo de la última conexión entre el dispositivo de agente 120 y el nodo 110). El controlador remoto 1 puede seleccionar también más de un dispositivo de agente 120 y ejecutar las siguientes etapas para cada dispositivo de agente seleccionado en paralelo o en secuencia: esta posibilidad permite alcanzar nodos 110 conectados únicamente a un dispositivo de agente, ocultando al administrador de red la complejidad de selección de dispositivo de agente.

En el bloque 802 el controlador remoto 1 ordena al dispositivo de agente 120 entrar en contacto con el nodo específico 110 en la dirección de IP especificada. Si se requiere (es decir si un nodo que se alcanza tiene una dirección de MAC diferente de la dirección de MAC especificada), el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) invoca un procedimiento de evasión de conflictos de IP, como se describe en mayor detalle a continuación con referencia a la figura 12.

Si se requiere, (es decir si la dirección de IP especificada no está incluida en ningún identificador de IP de subred de las interfaces del dispositivo de agente 120 y/o si la dirección de IP especificada corresponde a la dirección de IP de la interfaz de dispositivo de agente), en el bloque 802 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) puede invocar también un mecanismo de evasión de conflictos de subred, como se describe en mayor detalle a continuación con referencia a la figura 13.

En el bloque 803 el controlador remoto 1 (o el dispositivo de agente 120) comprueba si un nodo que tiene un conflicto de IP con el nodo específico 110 se ha descubierto durante alguna ejecución del procedimiento de evasión de conflictos de IP.

En caso positivo, en el bloque 806 el controlador remoto 1 añade las direcciones de IP y de MAC del nodo en conflicto en la primera sección 900 de la base de datos 14 en la lista de “nodos descubiertos”.

De todas maneras, en el bloque 804 el controlador remoto 1 (o el dispositivo de agente 120) comprueba si el nodo específico 110 con la dirección de IP y de MAC especificadas se ha alcanzado.

En caso negativo, en el bloque 807 el controlador remoto 1 añade las direcciones de IP y de MAC especificadas en la primera sección 900 de la base de datos 14 en la lista de “nodos no alcanzables”.

En caso positivo, en el bloque 805 el controlador remoto 1 añade las direcciones de IP y de MAC especificadas en la primera sección 900 de la base de datos 14 en la lista de “nodos disponibles”.

La Figura 9 muestra una segunda realización de un procedimiento de descubrimiento, haciendo uso de únicamente

direcciones de IP.

En el bloque 901 el administrador de red especifica al controlador remoto 1 únicamente la dirección de IP de un nodo específico 110 a descubrir.

La siguiente etapa depende de las capacidades del dispositivo de agente 120.

En la comprobación 902, se comprueba (mediante el controlador remoto o el dispositivo de agente 120) si el dispositivo de agente 120 soporta un protocolo de traducción para resolución de direcciones de IP en direcciones de MAC, como por ejemplo el ARP.

En caso negativo, en el bloque 903 el dispositivo de agente 120 intenta entrar en contacto con el nodo específico usando la dirección de IP especificada.

En el bloque 904, el controlador remoto 1 (o el dispositivo de agente 120) comprueba si un nodo 110 con la dirección de IP especificada se ha alcanzado.

En caso negativo, en el bloque 905 el controlador remoto 1 añade la dirección de IP especificada en la primera sección 900 de la base de datos 14 en la lista de “nodos no alcanzables” y el procedimiento finaliza.

En caso positivo, en el bloque 906 el controlador remoto 1 añade la dirección de IP especificada y la dirección de MAC, según se recuperan durante la conexión con el nodo 110, en la primera sección 900 de la base de datos 14 en la lista de “nodos disponibles”.

Cuando la comprobación en el bloque 902 es positiva (es decir el dispositivo de agente 120 soporta un protocolo de traducción), en el bloque 907 el dispositivo de agente 120 envía una solicitud adecuada (por ejemplo solicitud ARP) a la LAN 100 para traducir la dirección de IP especificada a una dirección de MAC correspondiente, de acuerdo con el protocolo de traducción.

En el bloque 908 el controlador remoto 1 comprueba si se ha recibido alguna dirección de MAC como respuesta a la solicitud.

Si no se recibe dirección de MAC, en el bloque 905 el controlador remoto 1 añade la dirección de IP especificada en la primera sección 900 de la base de datos 14 en la lista de “nodos no alcanzables” y el procedimiento finaliza.

Si únicamente se recibe una dirección de MAC, en el bloque 906 el controlador remoto 1 añade la dirección de IP especificada y las direcciones de MAC recibidas en la primera sección 900 de la base de datos 14 en la lista de “nodos disponibles”.

Si se recibe más de una dirección de MAC, en el bloque 909 el controlador remoto 1 añade la dirección de IP especificada con la pluralidad de direcciones de MAC recibidas asociadas en la primera sección 900 de la base de datos 14 en la lista de “nodos descubiertos”. En este caso, el controlador remoto 1 (automáticamente o bajo el control del administrador de red) tendrá que resolver el conflicto de IP, como se explica por ejemplo en lo sucesivo.

La Figura 10 muestra una tercera realización de un procedimiento de descubrimiento, haciendo uso de únicamente direcciones de MAC de los nodos 110 a descubrir.

En el bloque 1001 el administrador de red especifica al controlador remoto 1 únicamente la dirección de MAC de un nodo específico 110 a descubrir.

La siguiente etapa depende de las capacidades del dispositivo de agente 120.

En la comprobación 1002, se comprueba (mediante el controlador remoto o el dispositivo de agente 120) si el dispositivo de agente 120 soporta un protocolo de traducción para resolución de direcciones de MAC en direcciones de IP, como por ejemplo el RARP.

En caso negativo, en el bloque 1003 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) intenta alcanzar el nodo específico haciendo una primera exploración de direcciones de IP. La exploración puede realizarse aplicando el procedimiento descrito a continuación con referencia a la figura 11 y deteniéndolo cuando se alcanza un nodo con la dirección de MAC especificada.

En el bloque 1004, el controlador remoto 1 comprueba si el nodo específico con la dirección de MAC especificada se ha encontrado durante la primera exploración.

En caso positivo, en el bloque 1012 el controlador remoto 1 añade la dirección de MAC especificada con la dirección de IP asociada en la lista de “nodos disponibles” de la primera sección 900 de la base de datos 14 y el procedimiento finaliza.

En caso negativo, antes de considerar el nodo como no alcanzable, en los bloques 1005 y 1006, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) ejecuta preferentemente una segunda exploración intentando alcanzar todas las direcciones de IP satisfactoriamente alcanzadas mediante el dispositivo de agente 120, durante la primera exploración del bloque 1003.

Estas direcciones de IP están contenidas en una lista de IP creada mediante el dispositivo de agente 120 durante la primera exploración, que incluye la terna IP-SUBRED-INTERFAZ (es decir, dirección de IP, identificador de subred e identificador de interfaz) que indica, para cada dirección de IP alcanzada mediante el dispositivo de agente 120 durante la primera exploración, el identificador de la subred y el identificador de la interfaz de dispositivo de agente en la que se ha alcanzado la dirección de IP.

En el bloque 1005 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) selecciona una terna IP-SUBRED-INTERFAZ de dicha lista de IP.

En el bloque 1006 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) intenta entrar en contacto con la dirección de IP incluida en la terna seleccionada en el bloque 1005 a través de la interfaz incluida en dicha terna invocando, si se requiere, el procedimiento de evasión de conflictos de subred y, opcionalmente, el procedimiento de evasión de conflictos de IP, de acuerdo con los procedimientos detallados en lo sucesivo.

La segunda exploración realizada en los bloques 1005 y 1006 es útil para alcanzar un nodo identificado mediante la dirección de MAC específica que puede estar oculta por una dirección de IP contenida en la lista de IP, debido a un conflicto de IP.

En el bloque 1007, el controlador remoto 1 (o el dispositivo de agente 120) comprueba si se ha alcanzado un nodo.

En caso positivo, en el bloque 1012 el controlador remoto 1 añade la dirección de MAC especificada con la correspondiente dirección de IP en la primera sección 900 de la base de datos 14 en la lista de “nodos disponibles” y el procedimiento finaliza.

En caso negativo, en el bloque 1008 el controlador remoto 1 (o el dispositivo de agente 120) comprueba si todas las ternas IP-SUBRED-INTERFAZ de dicha lista de IP se han explorado.

En caso negativo, el procedimiento vuelve al bloque 1005.

En caso positivo (es decir, cuando no se ha alcanzado ningún dispositivo con una dirección de IP incluida en la lista de IP y la dirección de MAC especificada), en el bloque 1009 el controlador remoto 1 añade la dirección de MAC especificada en la primera sección 900 de la base de datos 14 en la lista de “nodos no alcanzables”.

En el caso positivo del bloque 1002 (es decir, cuando el dispositivo de agente soporta un protocolo de traducción para resolución de direcciones de MAC en direcciones de IP), en el bloque 1010 el controlador remoto 1 envía, a través del dispositivo de agente 120, una solicitud (por ejemplo solicitud RARP) en la LAN 100 para traducir la dirección de MAC especificada a una dirección de IP correspondiente.

En el bloque 1011 el controlador remoto 1 comprueba si se ha recibido alguna dirección de IP como respuesta a la solicitud enviada.

Si no se recibe dirección de IP, el procedimiento continúa en el bloque 1003.

Si únicamente se recibe una dirección de IP, en el bloque 1012 el controlador remoto 1 añade la dirección de MAC especificada con la dirección de IP recibida en la primera sección 900 de la base de datos 14 en la lista de “nodos disponibles”.

Si se recibe más de una dirección de IP (por ejemplo, cuando hay alias en una interfaz de un nodo 110 de modo que hay más de una dirección de IP asociada a tal interfaz o hay un caso de conflicto de MAC), en el bloque 1013 el controlador remoto 1 añade la dirección de MAC especificada con la pluralidad de direcciones de IP recibidas asociadas en la primera sección 900 de la base de datos 14 en la lista de “nodos descubiertos”. A continuación, el controlador remoto 1 (automáticamente o bajo el control del administrador de red) puede decidir, por ejemplo, usar indistintamente cualquiera de las direcciones de IP cada vez que necesite alcanzar el nodo o para elegir una específica para usar.

Ventajosamente, de acuerdo con la invención, se contempla también un procedimiento de descubrimiento basado en exploración, que puede implementarse automáticamente mediante el controlador remoto 1 sin requerir ninguna información desde el administrador de red.

De acuerdo con este procedimiento de descubrimiento basado en exploración, se considera una pluralidad de identificadores de subred. Los nodos 110 en la LAN 100 se descubren intentando entrar en contacto -a través de todas las interfaces de dispositivo de agente- todas las direcciones de IP (o una subparte seleccionada) que corresponden a tal pluralidad de identificadores de subred (es decir, intentando entrar en contacto con todas las posibles combinaciones de direcciones de IP obtenibles con los identificadores de subred).

La pluralidad de identificadores de subred preferentemente incluye los identificadores de subred asociados a las interfaces del dispositivo de agente 120 y, preferentemente, también una pluralidad de identificadores de subred, que corresponden a identificadores de subred típicos (conocidos preferentemente a priori) establecidos por defecto mediante diferentes fabricantes/distribuidores. Esta última característica permite extender ventajosamente la búsqueda a direcciones de IP, establecidas por defecto mediante diferentes fabricantes/distribuidores, que pueden pertenecer a una subred diferente de las cubiertas mediante las interfaces del dispositivo de agente.

La Figura 11 muestra una realización del procedimiento de descubrimiento basado en exploración de acuerdo con la invención.

En el bloque 1101, el dispositivo de agente 120 (bajo el control del controlador remoto 1) genera una lista de ID de subred y añade en dicha lista de ID de subred los identificadores de las subredes cubiertas mediante las interfaces de dispositivo de agente.

En el bloque 1102 el controlador remoto 1 envía al dispositivo de agente 120 una pluralidad de identificadores de subred, que corresponden a identificadores de subred típicos (preferentemente conocidos a priori) establecidos por defecto mediante diferentes fabricantes/distribuidores.

En el bloque 1103, el dispositivo de agente 120 los añade en la lista de ID de subred generada.

En el bloque 1104, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) selecciona de la lista de ID de subred generada un identificador de subred no explorado.

En el bloque 1105, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) selecciona una dirección de IP no explorada de entre todas las posibles direcciones de IP que corresponden al identificador de subred seleccionado.

En el bloque 1106, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) selecciona una interfaz de dispositivo de agente que no se ha intentado aún con la dirección de IP seleccionada. Preferentemente, la selección puede realizarse tal como para minimizar la distancia entre la dirección de IP seleccionada y el identificador de la subred que corresponde a la interfaz.

En el bloque 1107, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) intenta entrar en contacto con la dirección de IP seleccionada a través de la interfaz seleccionada. Si se requiere, se invocará el mecanismo de evasión de conflictos de subred, como se detalla en lo sucesivo.

En el bloque 1108, el controlador remoto 1 (o el dispositivo de agente 120) comprueba si se ha alcanzado un nodo.

En caso positivo, en el bloque 1109, el controlador remoto 1 añade las direcciones de IP y de MAC del nodo alcanzado en la primera sección 900 de la base de datos 14 en la lista de “nodos descubiertos”. Ventajosamente, los identificadores de subred y de interfaz se registran también. De hecho, puede ocurrir que se alcance una misma dirección de IP a través de diferentes interfaces, por ejemplo debido a que diferentes nodos conectados a diferentes interfaces están configurados con dirección de IP por defecto idéntica inicial.

De todas maneras, en el bloque 1110, el controlador remoto 1 (o el dispositivo de agente 120) comprueba si hay otras interfaces no intentadas del dispositivo de agente 120 para la dirección de IP seleccionada. En caso positivo, el procedimiento continúa en el bloque 1106. En caso negativo, en el bloque 1111, el controlador remoto 1 (o el dispositivo de agente 120) comprueba si hay otras direcciones de IP no exploradas para la subred seleccionada. En caso positivo, el procedimiento continúa en el bloque 1105. En caso negativo, en el bloque 1112, el controlador remoto 1 (o el dispositivo de agente 120) comprueba si hay otras subredes no exploradas. En caso positivo, el procedimiento continúa en el bloque 1104. En caso negativo, el procedimiento finaliza (es decir, todas las direcciones de IP de todas las subredes se han intentado a través de todas las interfaces del dispositivo de agente 120).

Ventajosamente, el procedimiento de descubrimiento basado en exploración de la figura 11 puede hacerse más eficaz si, antes de la ejecución de la exploración, se usa al menos una técnica para comprobar si es posible obtener

parejas de direcciones de IP/MAC para al menos parte de los nodos 110 de la LAN 100.

Ejemplos de tales técnicas son:

- uso de ping de difusión de acuerdo con la utilidad ping bien conocida en la técnica (como por ejemplo definida en el documento RFC 792);

- adoptar técnicas de análisis de paquetes de IP, u otras técnicas de exploración pasiva conocidas en la técnica para monitorizar el tráfico de la LAN y para descubrir la existencia de nodos;

- protocolos de descubrimiento de dispositivos bien conocidos, tales como UPnP (Conectar y Usar Universal, como por ejemplo descritos en el sitio web de internet www.upnp.org), Bonjour (como por ejemplo descrito en el sitio web http://developer.apple.com/opensource/), Interconexión Sin Necesidad de Configuración (como, por ejemplo, definido mediante el documento RFC 3927), o similares, que permitirían al dispositivo de agente 120 recibir mensajes específicos enviados mediante nodos que se auto-declaran, que soportan ellos mismos tales protocolos.

El uso de tales técnicas permite ventajosamente limitar el procedimiento de exploración a direcciones de IP no recuperadas a través de alguna de tales técnicas (las recuperadas pueden descubrirse usando el procedimiento de descubrimiento de la figura 8) y para conseguir cómo conocer acerca de alguna dirección de IP opcionalmente incluida en la LAN 100 pero no incluida en la lista de ID de subred generada en los bloques 1101-1103.

Una característica interesante de la invención es que el intervalo de direcciones de IP que el dispositivo de agente 120 puede acceder y detectar puede configurarse para aumentar el nivel de seguridad. De esta manera el administrador de red puede decidir qué subconjunto de nodos 110 es visible mediante el dispositivo de agente 120 y, como consecuencia, será gestionable a través del controlador remoto 1. El intervalo de dirección puede especificarse en diferentes técnicas bien conocidas, por ejemplo usando listas blancas o listas negras.

Se observa adicionalmente que incluso si en la realización de la figura 11 se exploran direcciones de IP considerando -para cada identificador de subred- todas las posibles direcciones de IP que corresponden a dicho identificador de subred y -para cada dirección de IP- todas las posibles interfaces de dispositivo de agente, la exploración puede llevarse a cabo considerando una secuencia de exploración diferente. Por ejemplo, las direcciones de IP pueden explorarse considerando -para cada interfaz de dispositivo de agente- los diversos identificadores de subred de la lista de ID de subred y -para cada identificador de subred- todas las posibles direcciones de IP que corresponden a dicho identificador de subred.

En una LAN 100 donde se despliegan múltiples nodos de distribuidor genéricos con su configuración por defecto, es muy probable que dos o más nodos estén asociados inicialmente a una misma dirección de IP, aunque tengan una dirección de MAC diferente. Este evento crea conflictos de IP de modo que ninguno de estos nodos puede alcanzarse apropiadamente mediante IP por el dispositivo de agente 120, de acuerdo con técnicas de interconexión convencionales.

Por esta razón, en una realización preferida, la invención proporciona un mecanismo que permite al dispositivo de agente 120 excluir todos los nodos con la misma dirección de IP excepto uno que tiene una dirección de MAC especificada y ponerse en contacto con él.

De acuerdo con este mecanismo, después de que se establece una conexión de túnel con el controlador remoto 1 mediante dispositivo de agente 120, cada vez que el controlador remoto 1 necesita conectar a un nodo específico de la LAN usando una dirección de IP y dirección de MAC específicas, se ejecuta ventajosamente un procedimiento de evasión de conflictos de IP mediante el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) para garantizar la conexión a la dirección de IP y dirección de MAC especificadas incluso en caso de que las direcciones de IP especificadas estén asociadas a múltiples direcciones de MAC.

La Figura 12 shows el procedimiento de evasión de conflictos de IP de acuerdo con una realización de la invención, en el que el dispositivo de agente 120 soporta el protocolo ARP, incluyendo la tabla ARP.

De acuerdo con el protocolo ARP, la tabla ARP del dispositivo de agente contendrá, para cada interfaz de dispositivo de agente, entradas representadas mediante parejas de direcciones de IP/MAC de los nodos 110 de la LAN 100. Estas entradas se actualizan cada vez que el dispositivo de agente envía solicitudes ARP en la LAN 100. De acuerdo con el protocolo ARP, el ARP puede contener únicamente una entrada cada dirección de IP. Por lo tanto, si más de un nodo responde a una solicitud ARP, la tabla ARP se actualiza con una pareja de dirección de IP/MAC que corresponde a únicamente uno de los nodos que responde (por ejemplo, el último nodo que contesta a la solicitud ARP).

En el bloque 1201 el dispositivo de agente 120, que necesita entrar en contacto con un nodo específico identificado mediante una dirección de IP especificada y una dirección de MAC especificada, envía (automáticamente o bajo el

control del controlador remoto 1) una solicitud ARP para traducir la dirección de IP especificada.

Después de enviar la solicitud ARP, en el bloque 1102 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) busca en su tabla ARP.

En el bloque 1203, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) comprueba si la tabla ARP incluye la dirección de IP especificada.

En caso positivo, en el bloque 1204 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) comprueba si la dirección de MAC recuperada, es decir la asociada en la tabla ARP a la dirección de IP especificada, es igual a la dirección de MAC especificada, es decir la que debería contactarse.

En caso positivo, en el bloque 1205 el dispositivo de agente (automáticamente o bajo el control del controlador remoto 1) intenta entrar en contacto con el nodo usando la dirección de IP especificada.

Existe diversas maneras bien conocidas en la técnica que el dispositivo de agente 120 puede usar para conectarse a un dispositivo específico tal como usar una solicitud de ping o creando un conector de TCP (Protocolo de Control de Transmisión) a la dirección de IP especificada, de acuerdo con técnicas bien conocidas en la técnica.

En el bloque 1206 el dispositivo de agente (automáticamente o bajo el control del controlador remoto 1) comprueba si el nodo se ha alcanzado. En caso positivo, el procedimiento finaliza. En caso negativo, en el bloque 1211 se devuelve un error específico y el procedimiento finaliza.

En el caso negativo del bloque 1203 (es decir, la tabla ARP no incluye la dirección de IP especificada) se devuelve un error específico y el procedimiento finaliza.

En el caso negativo del bloque 1204 (es decir la dirección de MAC recuperada no es igual a la dirección de MAC especificada), en el bloque 1208 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) registra el identificador de interfaz a través de la que recibió la respuesta a la solicitud ARP.

En el bloque 1209 el dispositivo de agente 120 borra en la tabla ARP la entrada en correspondencia con el identificador de interfaz registrado que contiene la dirección de IP especificada y la dirección de MAC recuperada.

En el bloque 1110 el dispositivo de agente 120 añade en la tabla ARP, en correspondencia con el identificador de interfaz registrado, una entrada ARP que contiene la dirección de IP especificada y la dirección de MAC especificada.

Desde el bloque 1110 el procedimiento continúa en el bloque 1205.

Las etapas en los bloques 1208 a 1210 permiten al dispositivo de agente entrar en contacto con el nodo identificado mediante la dirección de IP específica y la dirección de MAC específica, evitando interferencia con otros nodos en conflicto que tienen la misma dirección de IP pero diferente dirección de MAC.

Un uso periódico del procedimiento de evasión de conflictos de IP, también después de la configuración inicial de la LAN 100, permite ventajosamente al controlador remoto 1 eleve la advertencia al administrador de red cada vez que exista un conflicto de IP, por ejemplo generado por la conexión de un nuevo nodo en conflicto a la LAN 100, en un momento sucesivo a la configuración inicial.

De acuerdo con una realización preferida (no mostrada), cada vez que el procedimiento de evasión de conflictos de IP evita un conflicto a través de la ejecución de las etapas 1208 a 1210, las direcciones de IP y de MAC de los nodos en conflicto se añaden en la lista de “nodos descubiertos” incluida en la primera sección 900 de la base de datos 14 del controlador remoto 1 (como se explica, por ejemplo, en los bloques 803 y 806 de la figura 8).

Esto permite al controlador remoto 1 tener conocimiento de los nodos en conflicto de IP de la LAN 100 y ejecutar un mecanismo para resolver los conflictos de IP y garantizar las operaciones de protocolo de interconexión convencionales.

El mecanismo para resolver los conflictos de IP puede ejecutarse automáticamente mediante el controlador remoto 1 o bajo el control del administrador de red.

De acuerdo con una realización, el mecanismo de resolución de conflicto puede recopilar todas las direcciones de MAC de los nodos en conflicto y asignar a cada uno una dirección de IP específica, compatible con un plan de direccionamiento, usando el procedimiento de evasión de conflictos de IP como se ha descrito anteriormente.

Por ejemplo, si el nodo AA:AA:AA:AA:AA:AA, BB:BB:BB:BB:BB:BB, CC:CC:CC:CC:CC:CC tiene la misma dirección de IP 192.168.0.1, el mecanismo de resolución de conflicto sería:

- entrar en contacto con la dirección de IP 192.168.0.1 aplicando el procedimiento de evasión de conflictos para forzar la dirección de MAC AA:AA:AA:AA:AA:AA,
- cambiar la dirección de IP del dispositivo AA:AA:AA:AA:AA:AA de 192.168.0.1 a 192.168.0.101,
- entrar en contacto con la dirección de IP 192.168.0.1 aplicando la evasión de conflictos para forzar la dirección de MAC BB:BB:BB:BB:BB:BB,
- cambiar la dirección de IP del dispositivo BB:BB:BB:BB:BB:BB de 192.168.0.1 a 192.168.0.102,
- entrar en contacto con la dirección de IP 192.168.0.1 aplicando la evasión de conflictos para forzar la dirección de MAC CC:CC:CC:CC:CC:CC
- cambiar la dirección de IP del dispositivo CC:CC:CC:CC:CC:CC de 192.168.0.1 a 192.168.0.103

Después de esta secuencia, los tres nodos ya no están en conflicto.

Cuando el dispositivo de agente 120 tiene más de una interfaz, el mecanismo de resolución de conflicto de red puede usar un mecanismo de evasión de conflictos de subred (descrito en lo sucesivo) para entrar en contacto con cada nodo y asignará direcciones de IP que son coherentes con cada identificador de las subredes cubiertas mediante las interfaces del dispositivo de agente.

Se observa que, cuando un nodo 110 de la LAN 100 tiene una dirección de IP que no está incluida en ninguna subred de las interfaces del dispositivo de agente 120 o que es la misma de la interfaz de dispositivo de agente, ese nodo no sería alcanzable mediante el dispositivo de agente 120 de acuerdo con técnicas de red convencionales. Por esta razón, un aspecto de la invención es la introducción de un procedimiento de evasión de conflictos de subred que fuerza el dispositivo de agente 120 a entrar en contacto con una dirección de IP específica a través de una interfaz específica.

La Figura 13 muestra una realización del procedimiento de evasión de conflictos de subred para entrar en contacto con una dirección de IP especificada a través de una interfaz especificada.

En el bloque 1300 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) considera la dirección de IP especificada, es decir con la que tiene que entrar en contacto, y el identificador de la subred que corresponde a la interfaz especificada, es decir la interfaz a través de la que tiene que entrar en contacto con la IP especificada.

En el bloque 1301 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) comprueba si la dirección de IP especificada está cubierta mediante el identificador de subred considerado y si la dirección de IP de la interfaz especificada es diferente de la dirección de IP especificada.

En caso negativo, en el bloque 1302 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) compara la IP especificada con los identificadores de todas las subredes de todas las interfaces del dispositivo de agente 120.

En el bloque 1303 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) comprueba si hay alguna subred que incluya la dirección de IP especificada.

En caso positivo, en el bloque 1304, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) elimina la subred de la interfaz a la que la subred está asociada o desconecta tal interfaz. Esta etapa es útil para evitar el caso de tener dos interfaces de dispositivo de agente con una misma subred asociada.

De todas maneras, en el bloque 1305 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) asigna la subred que corresponde a la dirección de IP especificada a la interfaz especificada y asigna a la interfaz especificada una dirección de IP de tal subred, que es diferente de la dirección de IP especificada. Esta asignación puede hacerse de acuerdo con técnicas bien conocidas en la técnica.

En el bloque 1306, el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) intenta entrar en contacto con la dirección de IP especificada a través de la interfaz especificada.

Cuando se especifica también una dirección de MAC, en caso de conflicto de IP, el procedimiento de evasión de conflictos de IP puede invocarse en el bloque 1306 para alcanzar el nodo que tiene tanto la dirección de IP especificada como la dirección de MAC especificada.

En el bloque 1307 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) comprueba si el estado de cualquier interfaz (es decir, conectada/desconectada, dirección de IP, subred) se ha

modificado.

En caso negativo el procedimiento finaliza.

En caso positivo, en la etapa 1308 el dispositivo de agente 120 (automáticamente o bajo el control del controlador remoto 1) restaura el estado inicial de las interfaces y el procedimiento finaliza.

Se ha observado que cuando la dirección de IP especificada corresponde a la dirección de IP de la interfaz especificada, las acciones en el bloque 1305 asignarán a la interfaz especificada una dirección de IP temporalmente diferente. En este caso, pueden ocurrir desconexiones entre el controlador remoto 1 y el dispositivo de agente 120, cuando la interfaz especificada es la misma que la usada mediante la conexión del dispositivo de agente 120 del controlador remoto 1. Si esto ocurre, el dispositivo de agente 120 tendrá que re-establecer la conexión con el controlador remoto 1. Esto puede hacerse, por ejemplo, de dos maneras: 1) el dispositivo de agente 120 mantiene la nueva dirección de IP asignada para la interfaz especificada y re-establece una conexión; 2) el dispositivo de agente 120 conmuta continuamente entre la nueva dirección de IP asignada y la dirección de IP especificada, para entrar en contacto respectivamente con el nodo y el controlador remoto 1.

Como se ha indicado anteriormente, el controlador remoto 1 implementa una pluralidad de procedimientos de gestión (por ejemplo almacenados en la sección 930 de la base de datos 14) que permiten acceder, configurar, controlar y monitorizar los nodos de la LAN 100 de diferentes distribuidores y/o fabricantes. Un aspecto ventajoso de esta invención es la capacidad del controlador remoto 1 para identificar cualquier nodo 110 de la LAN 100 descubierto por la intermediación del dispositivo de agente 120 y asociarlo a un conjunto específico de procedimientos de gestión, adecuados para gestionar el nodo específico.

Por consiguiente, después de ejecutar un procedimiento de descubrimiento de acuerdo con cualquiera de las realizaciones descritas con referencia a la figuras 8 a 11, usando eventualmente el procedimiento de evasión de conflictos de IP y/o el procedimiento de evasión de conflictos de subred, el controlador remoto 1 identifica, por la intermediación del dispositivo de agente 120, los nodos descubiertos.

La Figura 14 muestra un procedimiento de identificación de acuerdo con una primera realización de la invención, basándose en la idea de tener un conocimiento a priori, para cada nodo 110 de la LAN 100 (por ejemplo identificado mediante su dirección de MAC), de un procedimiento de conexión correspondiente, que posibilita al controlador remoto 1 conectar apropiadamente, por la intermediación del dispositivo de agente 120, a tal nodo 110.

Esto, por ejemplo, puede implementarse usando la estructura de la base de datos 14 de la figura 4A, en la que hay una configuración a priori del contenido de la segunda sección 910 (que contiene una lista de identificadores de nodos (por ejemplo direcciones de MAC) asociado a parámetros caracterizadores de dispositivo tales como modelo, distribuidor, fabricante, versión de software, versión de hardware, versión de firmware y/o número de serie) y la cuarta sección 930 (que comprende una pluralidad de procedimientos de gestión, cada uno asociado a parámetros caracterizadores de dispositivo específicos tales como modelo, distribuidor, fabricante, versión de software, versión de hardware, versión de firmware y/o número de serie).

En el bloque 1401 de la figura 14, el controlador remoto 1 selecciona un nodo 110 de la lista de nodos contenida en la primera sección 900 de la base de datos 14 (según se rellena mediante el procedimiento de descubrimiento previamente ejecutado). Preferentemente, únicamente se tienen en cuenta los dispositivos clasificados como “disponibles” y, opcionalmente, “descubiertos”.

A continuación, en el bloque 1402 el controlador remoto 1 recupera el procedimiento de conexión específica requerido para acceder al nodo seleccionado y para autenticarse por él, usando el identificador de nodo (por ejemplo dirección de MAC) y uniendo la información almacenada en la segunda y cuarta secciones 910, 930 de la base de datos 14.

En el bloque 1403, el controlador remoto 1 ejecuta el procedimiento de conexión recuperada para autenticarse mediante el nodo.

Una vez autenticado, en el bloque 1404, el controlador remoto 1 recupera parámetros caracterizadores de dispositivo desde el nodo.

En el bloque 1405 el controlador remoto 1 comprueba si los parámetros recuperados corresponden a los parámetros caracterizadores de dispositivo almacenados en la segunda sección 910 de la base de datos 14.

En caso positivo el procedimiento finaliza. En caso negativo, en el bloque 1406 surge un error y el procedimiento finaliza.

Un ejemplo de este procedimiento se informa por fines de claridad:

- la primera sección 900 de la base de datos 14 contiene identificadores de nodo, entre los que la dirección de MAC AA:BB:CC:DD:EE:FF del nodo debe identificarse y configurarse;

- la tercera sección 920 de la base de datos 14 contiene parámetros de configuración para este nodo, por ejemplo CLAVE WEP 1234567890 y DIRECCIÓN DE IP 192.168.1.1; para aplicarse al dispositivo, debe usarse el procedimiento específico distribuidor-modelo correcto, por lo tanto deben identificarse el distribuidor, modelo y versión de firmware;

- la segunda sección 910 contiene una lista de todas las direcciones de MAC soportadas con el distribuidor relacionado, modelo e información de firmware (información que puede estar disponible gracias al acuerdo específico con los distribuidores específicos):

    o MAC AA:AA:AA:AA:AA:AA, asociada al distribuidor US Robotics, modelo usr808054, firmware 1.0.2;

    o MAC AA:AA:AA:AA:AA:EE, asociada al distribuidor US Robotics, modelo usr808054, firmware 4.0.1;

    o MAC AA:BB:CC:DD:EE:FF, asociada al distribuidor Netgear, modelo WG103, firmware 3.1.

- la cuarta sección 930 contiene una lista de procedimientos de gestión para conectar, configurar y monitorizar modelos específicos de nodos (esta lista puede ampliarse en tiempo de ejecución sin generar interrupción de servicio, permitiendo por lo tanto soportar virtualmente cada versión de firmware de cada modelo de cada distribuidor/fabricante):

    o Procedimiento de Conexión A, asociado al distribuidor USRobotics, modelo usr808054, firmware 1.x y 2.x;

    o Procedimiento de Conexión B, asociado al distribuidor USRobotics, modelo usr808054, firmware 4.x;

    o Procedimiento de Conexión C, asociado al distribuidor Netgear, modelo WG101, WG102, WG103, firmware 3.1;

    o Procedimiento de Configuración D, requerido para configurar la dirección de IP del distribuidor USRobotics, modelo usr808054, firmware 4.x;

    o Procedimiento de Configuración E, requerido para configurar la dirección de IP de los dispositivos del distribuidor Netgear, modelo WG101, WG102, WG103, firmware 3.1;

    o Procedimiento de Configuración F, requerido para configurar la WEP de los dispositivos del distribuidor Netgear, modelo WG101, WG102, WG103, firmware 3.1;

- bloque 1401: el controlador remoto 1 selecciona desde la primera sección 900 el identificador de MAC del nodo que debe identificarse en términos de distribuidor/modelo, por ejemplo la dirección de MAC AA:BB:CC:DD:EE:FF;

- bloque 1402: el controlador remoto 1 selecciona desde la segunda sección 910 la información asociada a AA:BB:CC:DD:EE:FF, es decir el distribuidor Netgear, modelo WG103, firmware 3.1;

- bloque 1403: el controlador remoto 1 selecciona, desde la cuarta sección 930, el Procedimiento de Conexión C, ya que corresponde al distribuidor Netgear, modelo WG103, firmware 3.1, y lo ejecuta para conectarse al dispositivo;

- bloque 1404: el controlador remoto 1 solicita parámetros de dispositivo para el dispositivo (esta solicitud se considera que es parte del Procedimiento de Conexión C); si los parámetros recuperados corresponden al distribuidor Netgear, modelo WG103, firmware 3.1, entonces el nodo está correctamente identificado (y sus parámetros, tales como dirección de IP y clave WEP pueden configurarse con, respectivamente, el Procedimiento de Configuración E y el Procedimiento de Configuración F).

La Figura 15 muestra un procedimiento de identificación de acuerdo con una segunda realización de la invención. Este procedimiento está basado en una estructura de la base de datos 14 de acuerdo con la realización de la figura 4B y en un conocimiento a posteriori del contenido de la segunda sección 910 de la base de datos 14 (que contiene una lista de identificadores de nodos (por ejemplo direcciones de MAC) asociados a parámetros caracterizadores de dispositivo tales como modelo, distribuidor, fabricante, versión de software, versión de hardware, versión de firmware, número de serie y similares). De hecho, la segunda sección 910 se rellena y actualiza durante la ejecución de este procedimiento de identificación.

En el bloque 1501 el controlador remoto 1 selecciona un nodo 110 de la lista de nodos contenida en la primera sección 900 de la base de datos 14 (según se rellena mediante el procedimiento de descubrimiento previamente

ejecutado). Preferentemente, únicamente se tienen en cuenta los dispositivos clasificados como “disponibles” y, opcionalmente, “descubiertos”.

A continuación, en el bloque 1502 el controlador remoto 1 comprueba si hay un procedimiento de conexión específica para el nodo seleccionado, usando el identificador de nodo (por ejemplo dirección de MAC) y uniendo la información almacenada en la segunda y cuarta secciones 910, 930 de la base de datos 14.

En caso positivo, se ejecutan los bloques 1503 a 1506, que corresponden a los bloques 1402 a 1405 de la figura 14.

En el caso positivo del bloque 1506, el procedimiento finaliza.

En caso negativo, en el bloque 1507 el controlador remoto elimina de la segunda sección 910 la asociación entre la dirección de MAC y los correspondientes parámetros de dispositivo, y el procedimiento continúa en el bloque 1502. Esta característica es ventajosa para revelar diferentes versiones de firmware de un modelo de nodo específico.

En el caso negativo del bloque 1502, el controlador remoto 1 selecciona desde la quinta sección 911 una secuencia de procedimientos de conexión que se supone que incluyen un procedimiento correcto para el nodo específico, incluso aunque no esté caracterizado. Esta elección se hace en el bloque 1508, de acuerdo con un criterio de selección predeterminado. Ventajosamente, el criterio de selección tiene por objeto minimizar el número de procedimientos de conexión a probar antes de conectar satisfactoriamente al nodo 110. Por ejemplo, el criterio de selección para un procedimiento de conexión puede ser el tiempo medio para que el procedimiento sea satisfactorio, la diferencia entre la dirección de MAC del nodo seleccionado y la dirección de MAC de nodos que ya se han asociado satisfactoriamente al procedimiento de conexión, o que son parte de una lista de procedimientos asociados a un distribuidor predeterminado que se ha especificado mediante el administrador de red como distribuidor para el nodo o nodos 110. Ventajosamente, la lista de secuencias almacenada en la sección 911 incluye una secuencia por defecto que contiene todos los procedimientos de conexión disponibles en la base de datos, la sección 930, incluso si esta solución no se optimizara.

En el bloque 1509, el controlador remoto 1 intenta los procedimientos de conexión de la secuencia seleccionada.

En el bloque 1510 el controlador remoto 1 comprueba si al menos un procedimiento de conexión es satisfactorio.

En caso positivo, el nodo 110 se considera caracterizado y en el bloque 1512 su identificador (por ejemplo la dirección de MAC) se inserta en la segunda sección 910 de la base de datos 14, asociada a los parámetros caracterizadores de dispositivo recuperados desde el propio nodo durante el procedimiento de conexión.

En el caso negativo del bloque 1510, en el bloque 1511 el controlador remoto 1 registra una advertencia que contiene todos los detalles del dispositivo no soportado.

Un ejemplo de esta segunda realización se informa por fines de claridad:

- la primera sección 900 de la base de datos 14 contiene los identificadores de nodo, entre los cuales la dirección de MAC AA:BB:CC:DD:EE:FF del nodo que debe identificarse y configurarse;
- la tercera sección 920 de la base de datos 14 contiene los parámetros de configuración, por ejemplo CLAVE WEP 1234567890 y DIRECCIÓN DE IP 192.168.1.1;
- la segunda sección 910 de la base de datos 14 está vacía, como para cada dirección de MAC especificada mediante el usuario, no hay disponibles parámetros de dispositivo (distribuidor, modelo, versión de firmware);
- la cuarta sección 930 de la base de datos 14 contiene procedimientos para conectar, configurar y monitorizar modelos específicos de puntos de acceso:
    - o Procedimiento de Conexión A, asociado al distribuidor USRobotics, modelo usr808054, firmware 1.x y 2.x;
    - o Procedimiento de Conexión B, asociado al distribuidor USRobotics, modelo usr808054, firmware 4.x;
    - o Procedimiento de Conexión C, asociado al distribuidor Netgear, modelo WG101, WG102, WG103, firmware 3.1;
    - o Procedimiento de Conexión D, asociado al distribuidor Netgear, modelo WG001, WG002, SK999, firmware 2;
    - o Procedimiento de Configuración E, requerido para configurar la dirección de IP del distribuidor USRobotics, modelo usr808054, firmware 4.x;

o Procedimiento de Configuración F, requerido para configurar la dirección de IP de los dispositivos del distribuidor Netgear, modelo WG101, WG102, WG103, firmware 3.1;

o Procedimiento de Configuración G, requerido para configurar la WEP de los dispositivos del distribuidor Netgear, modelo WG101, WG102, WG103, firmware 3.1;

- la sección 911 de la base de datos 14 contiene diferentes secuencias de procedimientos de conexión:

  o Secuencia 1: Procedimiento de Conexión A, Procedimiento de Conexión B;

  o Secuencia 2: Procedimiento de Conexión D, Procedimiento de Conexión C;

  o Secuencia 3: Procedimiento de Conexión A, Procedimiento de Conexión B, Procedimiento de Conexión C, que contiene todos los procedimientos de conexión;

Cada secuencia está también caracterizada por parámetros de métrica, por ejemplo el número de veces que se ha ejecutado, el número de conexiones establecidas y denegadas, el número medio de procedimientos de conexión intentados antes del éxito por cada intervalo de dirección de MAC y similares. Ya que este último es una medida de la capacidad de la propia secuencia para conectarse a un dispositivo cuyo MAC radica en un intervalo específico, y como se conoce por los expertos en la materia cada intervalo de MAC está asociado a un distribuidor específico, esta métrica puede medir la capacidad de una secuencia para conectarse a un distribuidor específico pero de modelo desconocido.

- bloque 1501: el controlador remoto 1 selecciona desde la sección 900 el identificador de MAC del nodo que debe identificarse en términos de distribuidor/modelo, por ejemplo AA:BB:CC:DD:EE:FF;

- bloque 1508: el controlador remoto 1 selecciona una secuencia desde la sección 911, para minimizar alguna métrica. Si esta métrica es el número medio de procedimientos de conexión intentados antes del éxito, como se ha detallado anteriormente, se elegiría la Secuencia 2: contiene procedimientos que tienen éxito con direcciones de MAC que radican en el intervalo de Netgear, como lo hace el MAC AA:BB:CC:DD:EE:FF;

- bloque 1509: el controlador multi-distribuidor selecciona, desde la sección 930, el Procedimiento de Conexión D, ya que corresponde al primer procedimiento de conexión de la secuencia elegida (Secuencia 2); el Procedimiento de Conexión D falla, ya que está relacionado con un modelo que es diferente del dispositivo cuyo MAC es AA:BB:CC:DD:EE:FF; a continuación el controlador remoto 1 selecciona, desde la sección 930, el segundo procedimiento de la Secuencia 2, que es el Procedimiento de Conexión C, y lo ejecuta; ya que el distribuidor/modelo/versión del dispositivo corresponde a los soportados por el Procedimiento de Conexión C, el procedimiento tiene éxito y se recupera la caracterización AA:BB:CC:DD:EE:FF del dispositivo: distribuidor Netgear, modelo WG103, firmware 3.1;

- bloque 1512: como el Procedimiento de Conexión C tuvo éxito, el controlador multi-distribuidor puede asociar el MAC del dispositivo AA:BB:CC:DD:EE:FF distribuidor Netgear, modelo WG103, firmware 3.1, en la sección 910 de la base de datos;

- después de este procedimiento, el controlador remoto 1 podrá identificar el dispositivo AA:BB:CC:DD:EE:FF siguiendo las etapas a priori: 1503 a 1505.

Ventajosamente, el procedimiento de identificación de la figura 15 puede hacerse más eficaz si, antes de la ejecución del procedimiento, al menos una de una de las técnicas anteriormente mencionadas con referencia al procedimiento de descubrimiento de exploración (por ejemplo, UPnP, Bonjour, Interconexión Sin Necesidad de Configuración) se usa para comprobar si es posible obtener parejas de direcciones de IP/MAC junto con algún parámetro caracterizador de dispositivo (por ejemplo distribuidor) para al menos parte de los nodos 110 de la LAN 100.

Esto permitiría al controlador remoto 1 (o al dispositivo de agente 120) tener un conocimiento a priori de algunos parámetros de dispositivo que pueden usarse en el bloque 1508 para optimizar la selección de una secuencia apropiada de procedimientos de conexión.

Después de ejecutar un procedimiento de descubrimiento de acuerdo con cualquiera de las realizaciones descritas con referencia a la figuras 8 a 11, y un procedimiento de identificación de acuerdo con cualquiera de las realizaciones descritas con referencia a la figuras 14 y 15, el controlador remoto 1 está listo para usarse mediante el administrador de red para ejecutar las operaciones de gestión en los nodos 110. Estas operaciones pueden aplicarse mediante el administrador de red a nodos únicos 110, a un subconjunto de los nodos 110 de la LAN 100, o a todos los nodos 110 de la LAN 100. En cualquier caso, el administrador de red puede ejecutar estas operaciones a través de la interfaz de usuario del controlador remoto 18. Cuando el administrador de red desea gestionar un nodo 110, puede ejecutarse el siguiente procedimiento:

- el administrador de red inicia la interfaz de usuario del controlador remoto 18 (por ejemplo, sitio web, aplicación de tableta, etc.);

- el administrador de red proporciona parámetros de autenticación;

- el administrador de red selecciona el nodo que desea gestionar, entre la lista de “nodos disponibles” (cuadro 901 de la primera sección 900 de la base de datos 14, mostrado en la figura 5A) proporcionada mediante el controlador remoto 1;

- el administrador de red cambia uno o más parámetros de configuración del nodo seleccionado (por ejemplo la dirección de IP y/o el SSID);

- el controlador remoto 1 graba los nuevos parámetros de configuración en la base de datos 14 (tercera sección 920 mostrada en la figura 4), en asociación al modo seleccionado;

- el administrador de red confirma la nueva configuración;

- usando la información contenida en las secciones 910 y 930 de la base de datos 14, el controlador remoto 1, selecciona el procedimiento de configuración de distribuidor/modelo específico para usarse para configurar el nodo seleccionado;

- el controlador remoto 1 ejecuta el procedimiento de configuración de distribuidor/modelo específico para configurar el nodo y, cuando la ejecución está completada, devuelve una confirmación al administrador de red.

Una secuencia similar puede ejecutarse en caso de operaciones de monitorización.

Como es evidente a partir de la descripción anterior, la invención en los diversos aspectos de la misma permite conseguir una pluralidad de ventajas.

Una innovación crucial de la invención propuesta es el hecho de que no se requiere desplegar ningún software en los nodos 110 a gestionar, o suponer ningún procedimiento o comportamiento específico, para hacerla gestionable mediante el controlador remoto 1. Esto es posible gracias a la intermediación del dispositivo de agente 120, que inicia el contacto con el controlador remoto 1 y establece una conexión de túnel con él, y a los procedimientos de descubrimiento e identificación que posibilitan que el controlador remoto descubra qué nodos 110 están presentes en la LAN 100 y para identificar los parámetros caracterizadores de dispositivo (tales como fabricante/distribuidor, tipo, modelo, versión de hardware, versión de firmware, versión de software, número de serie, dirección de MAC y similares) de tales nodos, que posibilitan al controlador remoto 1 gestionar cada dispositivo usando procedimientos y protocolos de distribuidor/fabricantes específicamente conocidos.

Las interfaces propietarias disponibles en la técnica conocidas, tales como HTTP, HTTPS, CLI, SSH, ficheros de configuración, que se soportan e implementan de manera diferente mediante diferentes distribuidores/fabricantes, pueden usarse por lo tanto mediante el controlador remoto 1 para conectar, controlar, configurar y monitorizar los nodos, incluso cuando los nodos no se fabrican para gestionarse de manera central, sin la necesidad de modificar el software/firmware de tales nodos, o requerir algún comportamiento específico de los nodos distinto a las interfaces expuestas convencionales o propietarias.

Cualquier nodo, que provenga de un distribuidor/fabricante genérico, incluido en un dispositivo de red de calidad de cliente de bajo coste, puede gestionarse mediante el sistema de gestión remota de la invención.

Se observa además que un aspecto desafiante de usar nodos que provienen de distribuidores/fabricantes genéricos es que normalmente provienen de la fábrica con una dirección de IP integrada común. Esto significa que cada vez que se inserta un nuevo nodo en la LAN, es muy probable que surjan conflictos de direcciones de IP.

Gracias al procedimiento de evasión de conflictos de IP y al procedimiento de evasión de conflictos de subred de la invención, los conflictos de direcciones IP pueden gestionarse de manera central mediante el controlador remoto 1, sin la necesidad de desplegar ningún software específico en los nodos 110 a gestionar ni suponer ningún procedimiento o comportamiento específico para los nodos.

Una gestión central de conflictos de direcciones de IP garantiza también que se cumplan las políticas específicas establecidas mediante el administrador de red.

Esto es ventajoso con respecto a soluciones conocidas para conflictos de IP en los que los nodos necesitan configurarse para ejecutar algoritmos de auto-asignación (tales como por ejemplo el algoritmo de asociación de MAC-a-IP descrito mediante el documento US 7.852.819) y las direcciones de IP auto-asignadas pueden no ser compatibles con las políticas de red establecidas mediante el administrador de red.

**REIVINDICACIONES**

1. Método de gestión remota en una red (2, 100), comprendiendo la red (2, 100) una pluralidad de nodos (110) a gestionar mediante un controlador remoto (1) y al menos un dispositivo de agente (120), estando el al menos un dispositivo de agente (120) en un número inferior a la pluralidad de nodos (110), en donde:

- el al menos un dispositivo de agente (120) hace un contacto inicial con el controlador remoto (1) para autenticarse mediante el controlador remoto (1) y para establecer una conexión con el controlador remoto (1);
- una vez que se establece la conexión, el controlador remoto (1) ejecuta un procedimiento de descubrimiento por la intermediación del al menos un dispositivo de agente (120) para descubrir la pluralidad de nodos (110);
- una vez ejecutado el procedimiento de descubrimiento, el controlador remoto (1) ejecuta un procedimiento de identificación por la intermediación del al menos un dispositivo de agente (120) para identificar los nodos descubiertos (110), incluyendo la identificación de al menos un parámetro caracterizador seleccionado de entre: modelo, distribuidor, fabricante, versión de software, versión de hardware, versión de firmware, número de serie y dirección de MAC, en donde en el procedimiento de identificación el controlador remoto (1):

  a) selecciona un nodo específico (110) desde los nodos descubiertos (110);
  b) recupera desde una base de datos (14) del controlador remoto (1) que comprende una pluralidad de procedimientos de conexión (931) un procedimiento de conexión específica para conexión al nodo específico (110);
  c) usa el procedimiento de conexión específica recuperado para conectarse al nodo específico (110), por la intermediación del al menos un dispositivo de agente (120) y para obtener desde el nodo específico (110) dicho al menos un parámetro caracterizador;

- cuando la base de datos (14) no incluye el procedimiento de conexión específica asociado al nodo específico (110), el procedimiento de identificación incluye intentar en secuencia procedimientos de conexión de una secuencia de procedimientos de conexión para conectarse al nodo específico (110) hasta que se establece satisfactoriamente la conexión y dicho al menos un parámetro caracterizador se obtiene del nodo específico, seleccionándose la secuencia de procedimientos de conexión de acuerdo con un criterio de selección predeterminado;
- la base de datos (14) comprende una sección (930) que comprende una pluralidad de procedimientos de gestión, cada uno asociado a una instancia específica de dicho al menos un parámetro caracterizador, y
- el controlador remoto (1) gestiona cada uno de los nodos descubiertos e identificados (110) por la intermediación del al menos un dispositivo de agente (120), recuperando desde la base de datos (14) los procedimientos de gestión que están asociados en la base de datos (14) a la instancia que corresponde a al menos un parámetro caracterizador, como se obtiene desde el nodo (110) por medio de dicho procedimiento de identificación.

2. Método de acuerdo con la reivindicación 1, en el que la conexión establecida con el controlador remoto (1) es una conexión de túnel.

3. Método de acuerdo con la reivindicación 2, en el que la conexión de túnel se establece mediante el al menos un dispositivo de agente (120) de acuerdo con un procedimiento de tunelización que incluye la etapa de intentar en secuencia una pluralidad de protocolos de tunelización predeterminados para establecer la conexión de túnel con el controlador remoto (1) hasta que se establece satisfactoriamente una conexión de túnel.

4. Método de acuerdo con la reivindicación 3, en el que la pluralidad de protocolos de tunelización predeterminados se intentan en secuencia siguiendo un criterio de selección adaptado para minimizar recursos requeridos en el al menos un dispositivo de agente (120) y/o en el controlador remoto (1) para ejecutar los protocolos de tunelización.

5. Método de acuerdo con la reivindicación 1, en el que el procedimiento de descubrimiento incluye intentar establecer una conexión con la pluralidad de nodos (110), por la intermediación del al menos un dispositivo de agente (120), usando la dirección de IP y/o la dirección de MAC predeterminadas, o usando un procedimiento de exploración que explora una multitud predeterminada de direcciones de IP.

6. Método de acuerdo con la reivindicación 5, en el que la multitud de direcciones de IP predeterminadas comprenden direcciones de IP incluidas en al menos una subred que corresponde a al menos una interfaz del al menos un dispositivo de agente (120), y/o direcciones de IP genéricas que corresponden a direcciones de IP establecidas por defecto por fabricantes y/o distribuidores predeterminados.

7. Método de acuerdo con la reivindicación 5, en el que cuando el al menos un dispositivo de agente (120) comprende más de una interfaz, el procedimiento de exploración se ejecuta para cada interfaz.

8. Método de acuerdo con la reivindicación 1, en el que, cuando tiene que establecerse una conexión a un nodo específico (110) con una dirección de IP y una dirección de MAC especificadas, y en caso de conflicto de dirección de IP entre el nodo específico (110) y al menos otro nodo (110) de la pluralidad de nodos (110), el al menos un

dispositivo de agente (120) ejecuta un procedimiento de evasión de conflicto de IP haciendo uso del protocolo ARP y de la tabla ARP, comprendiendo el procedimiento de evasión de conflictos de IP:

i. enviar en la red (2, 100) una solicitud de acuerdo con el protocolo ARP para traducir la dirección de IP especificada a una dirección de MAC;
ii. después de ejecutar i., comprobar si la tabla ARP incluye la dirección de IP especificada;
iii. en caso positivo de ii., comprobar si la dirección de IP especificada está asociada en la tabla ARP a la dirección de MAC especificada;
iv. en caso positivo de iii., intentar establecer una conexión con el nodo específico (110) usando la dirección de IP especificada;
v. en caso negativo de iii., modificar la tabla ARP para asociar la dirección de IP especificada a la dirección de MAC especificada, a continuación intentar establecer una conexión con el nodo específico (110) usando la dirección de IP especificada.

9. Método de acuerdo con la reivindicación 1, en el que, cuando tiene que establecerse una conexión a una dirección de IP especificada a través de una interfaz especificada del al menos un dispositivo de agente (120), y en caso de conflicto de dirección de IP entre la dirección de IP especificada y la dirección de IP de la interfaz especificada y/o en caso de que la dirección de IP especificada no esté incluida en una subred que corresponde a la interfaz especificada, el al menos un dispositivo de agente (120) ejecuta un procedimiento de evasión de conflictos de subred que comprende:

I. comprobar si la dirección de IP especificada está incluida en la subred que corresponde a la interfaz especificada y si la dirección de IP especificada es diferente de la dirección de IP de la interfaz especificada,
II. en caso afirmativo de I., el al menos un dispositivo de agente (120) intenta establecer una conexión usando la dirección de IP especificada,
III. en caso negativo de I., el al menos un dispositivo de agente (120) asigna temporalmente a la interfaz especificada tanto una subred que incluye la dirección de IP especificada como una dirección de IP incluida en dicha subred, que es diferente de la dirección de IP especificada.

10. Método de acuerdo con la reivindicación 9, en el que, cuando el al menos un dispositivo de agente (120) comprende una pluralidad de interfaces, la etapa III comprende también una etapa de no hacer uso temporalmente de cualquier otra interfaz de la pluralidad de interfaces, distinta de la interfaz especificada, que corresponde a una subred que incluye la dirección de IP especificada.

11. Un sistema de gestión remota (10) que comprende un controlador remoto (1) y una red (2, 100), comprendiendo la red (2, 100) una pluralidad de nodos (110) a gestionar mediante el controlador remoto (1) y al menos un dispositivo de agente (120), estando el al menos un dispositivo de agente (120) en un número inferior a la pluralidad de nodos (110), **caracterizado por que** el controlador remoto (1) y el al menos un dispositivo de agente (120) comprenden medios de hardware y/o software y/o firmware adaptados para llevar a cabo el método de acuerdo con cualquiera de las reivindicaciones 1 a 10.

12. Un programa informático adaptado para llevar a cabo las etapas con respecto al controlador remoto (1) en el método de acuerdo con cualquiera de las reivindicaciones 1 a 10.

13. Un programa informático adaptado para llevar a cabo las etapas con respecto al dispositivo de agente (120) en el método de acuerdo con cualquiera de las reivindicaciones 1 a 10.

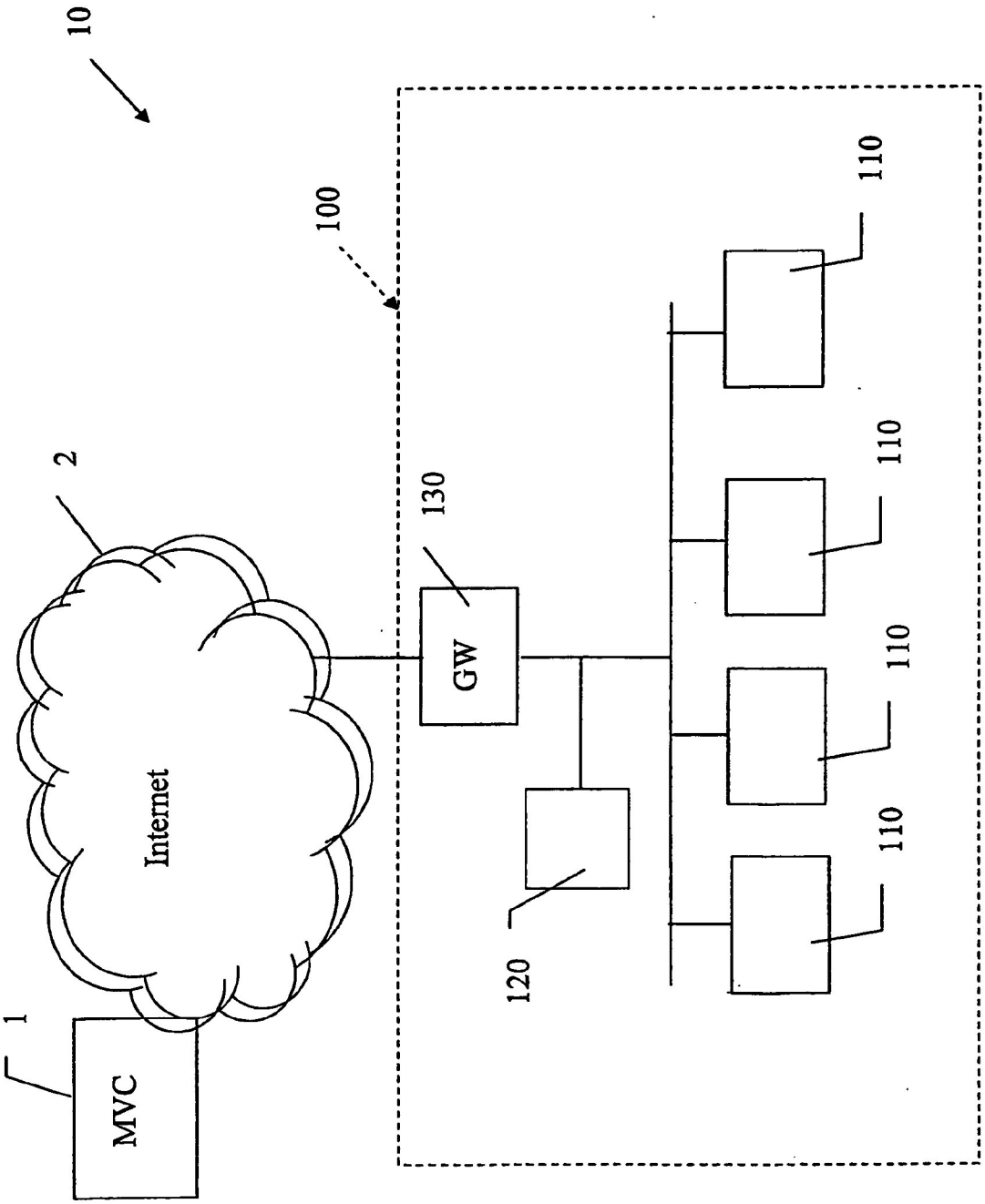


Fig. 1

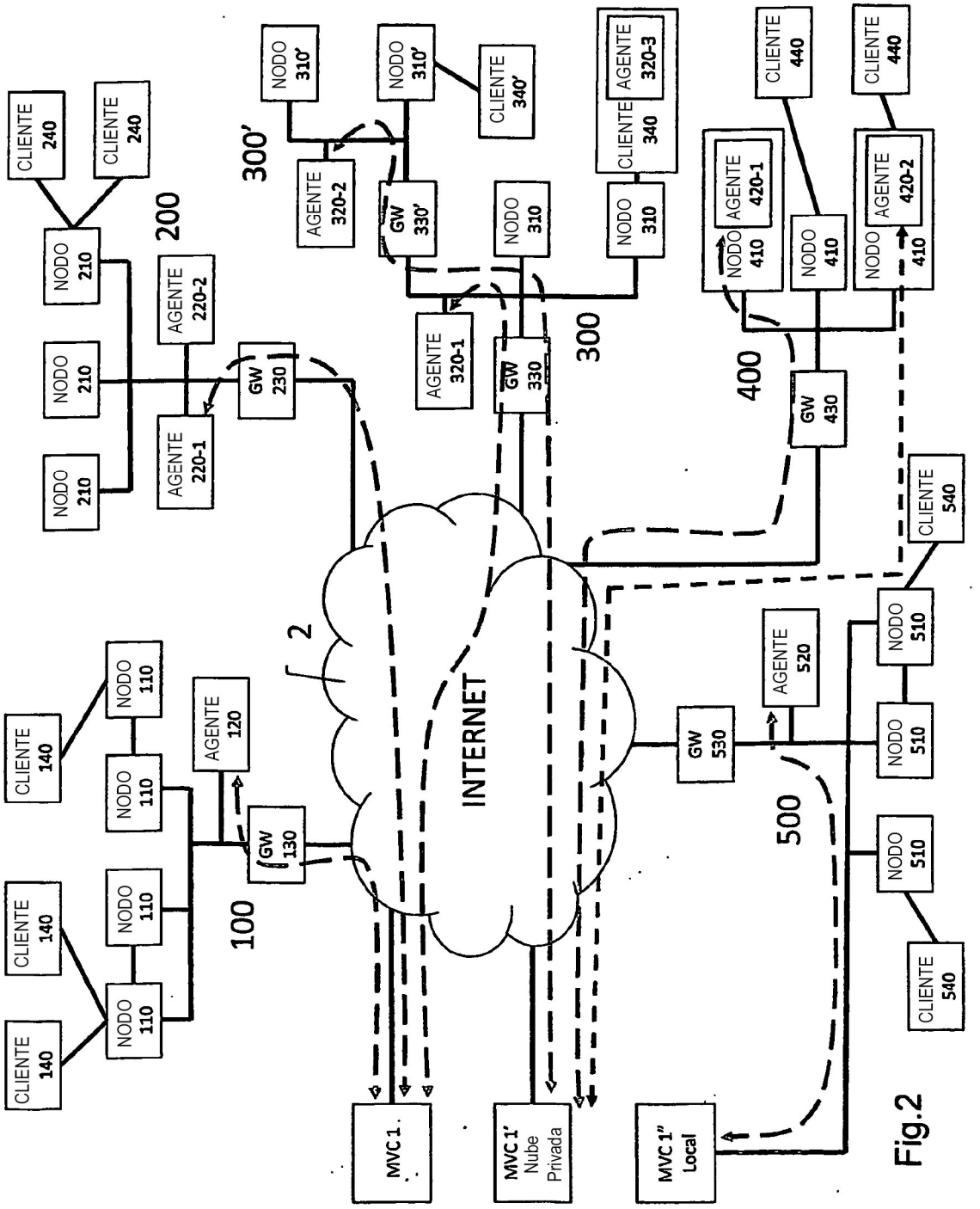
INTERNET
2
100
200
300
300'
400
500
CLIENTE 140
NODO 110
AGENTE 120
GW 130
CLIENTE 240
NODO 210
AGENTE 220-1
AGENTE 220-2
GW 230
NODO 310'
AGENTE 320-2
GW 330'
CLIENTE 340'
AGENTE 320-1
GW 330
NODO 310
CLIENTE 340
AGENTE 320-3
NODO 410
AGENTE 420-1
AGENTE 420-2
CLIENTE 440
GW 430
CLIENTE 540
NODO 510
AGENTE 520
GW 530
MVC 1
MVC 1' Nube Privada
MVC 1" Local

Fig.2

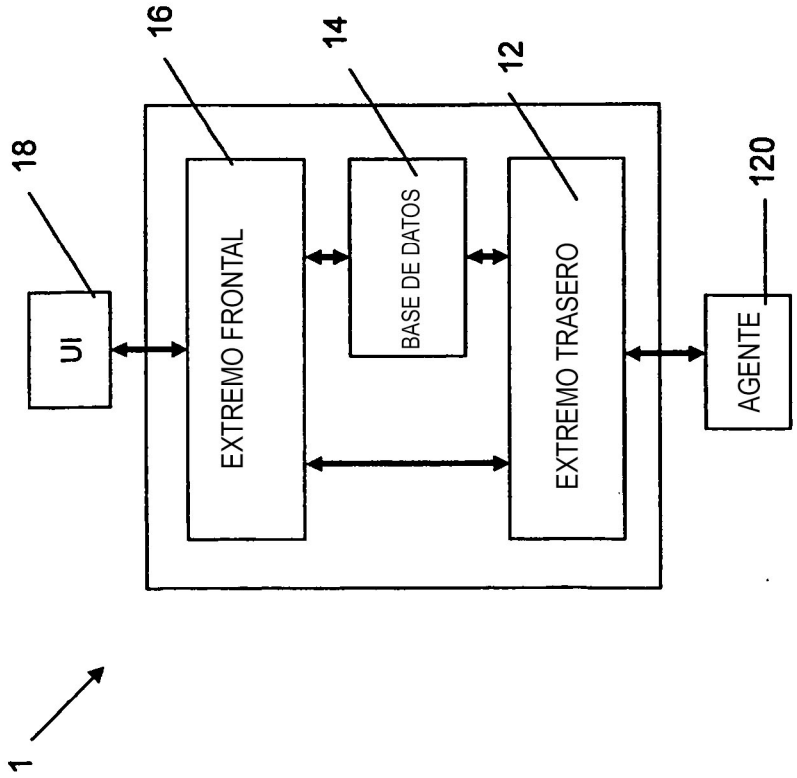
16
14
12
18
120
UI
EXTREMO FRONTAL
BASE DE DATOS
EXTREMO TRASERO
AGENTE
1

Fig.3

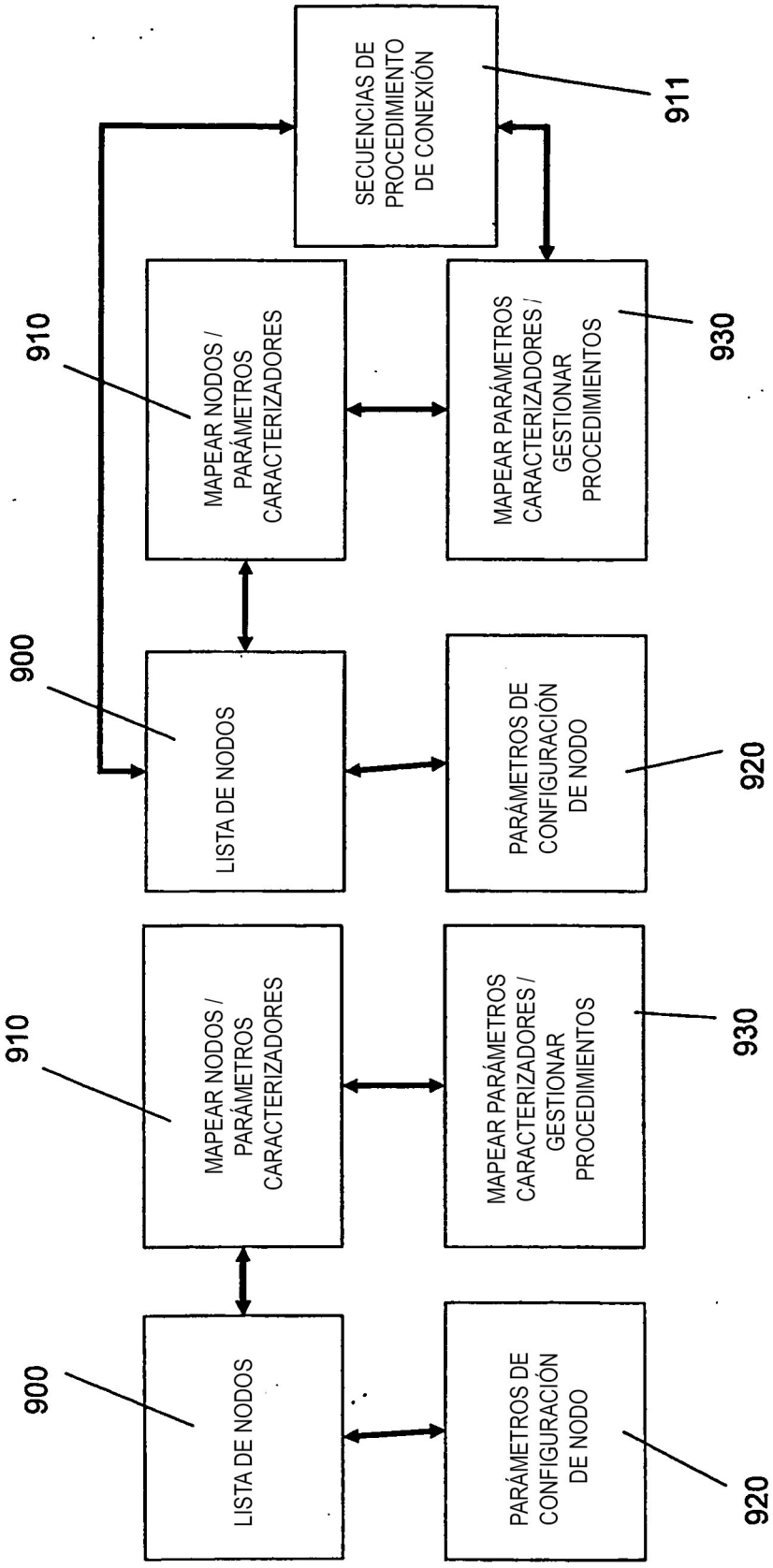
SECUENCIAS DE PROCEDIMIENTO DE CONEXIÓN
911
MAPEAR NODOS / PARÁMETROS CARACTERIZADORES
910
MAPEAR PARÁMETROS CARACTERIZADORES / GESTIONAR PROCEDIMIENTOS
930
LISTA DE NODOS
900
PARÁMETROS DE CONFIGURACIÓN DE NODO
920
MAPEAR NODOS / PARÁMETROS CARACTERIZADORES
910
MAPEAR PARÁMETROS CARACTERIZADORES / GESTIONAR PROCEDIMIENTOS
930
LISTA DE NODOS
900
PARÁMETROS DE CONFIGURACIÓN DE NODO
920

Fig.4B

Fig.4A

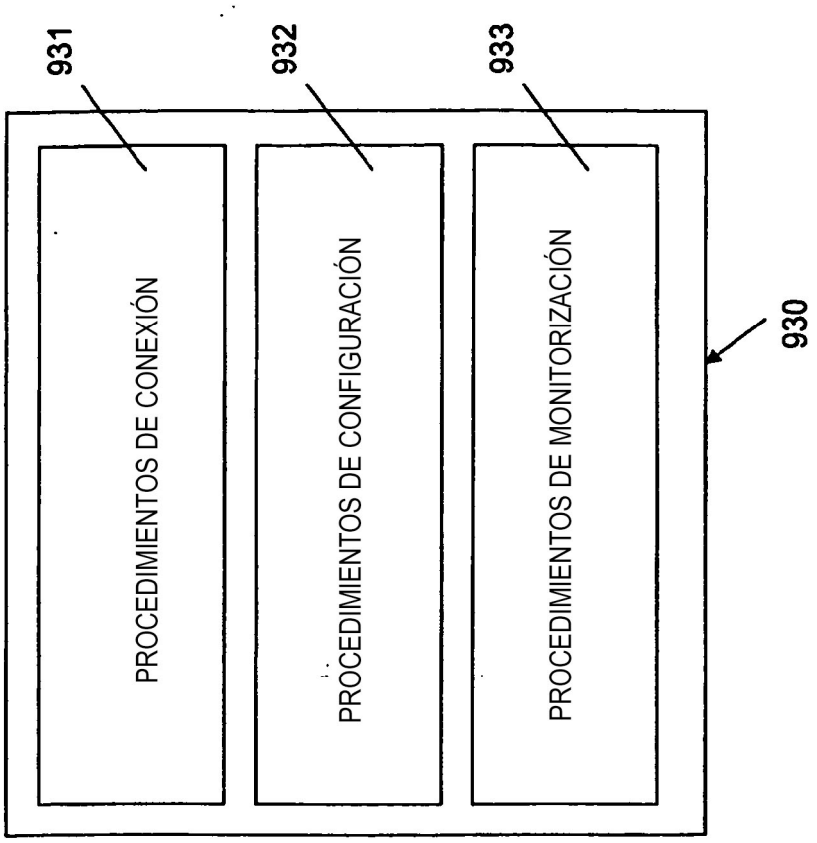
931
932
933
PROCEDIMIENTOS DE CONEXIÓN
PROCEDIMIENTOS DE CONFIGURACIÓN
PROCEDIMIENTOS DE MONITORIZACIÓN
930

Fig.5B

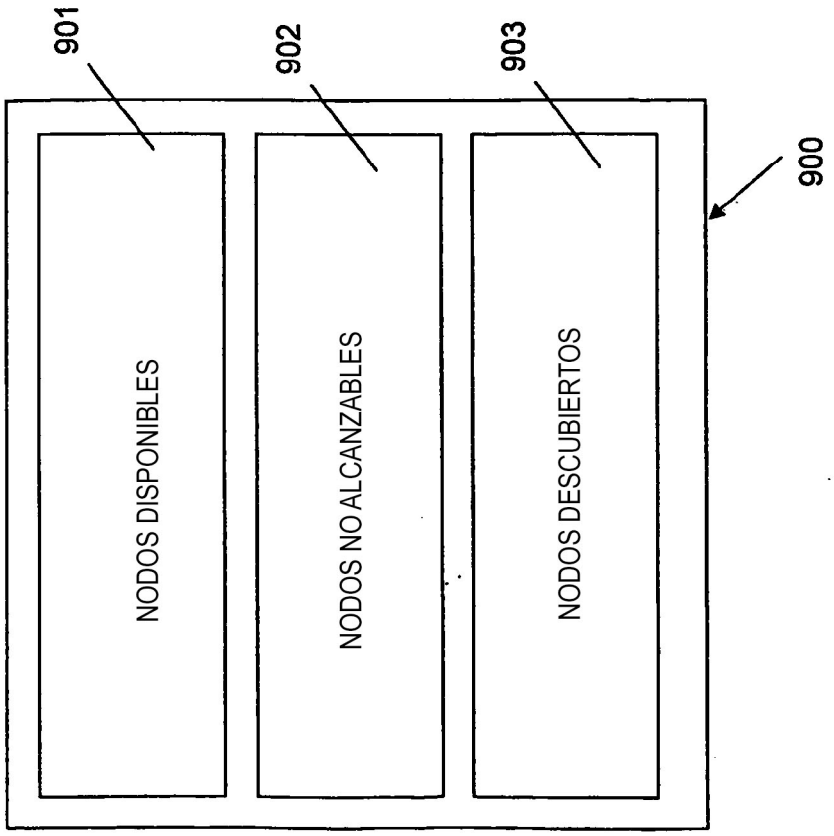
901
902
903
NODOS DISPONIBLES
NODOS NO ALCANZABLES
NODOS DESCUBIERTOS
900

Fig.5A

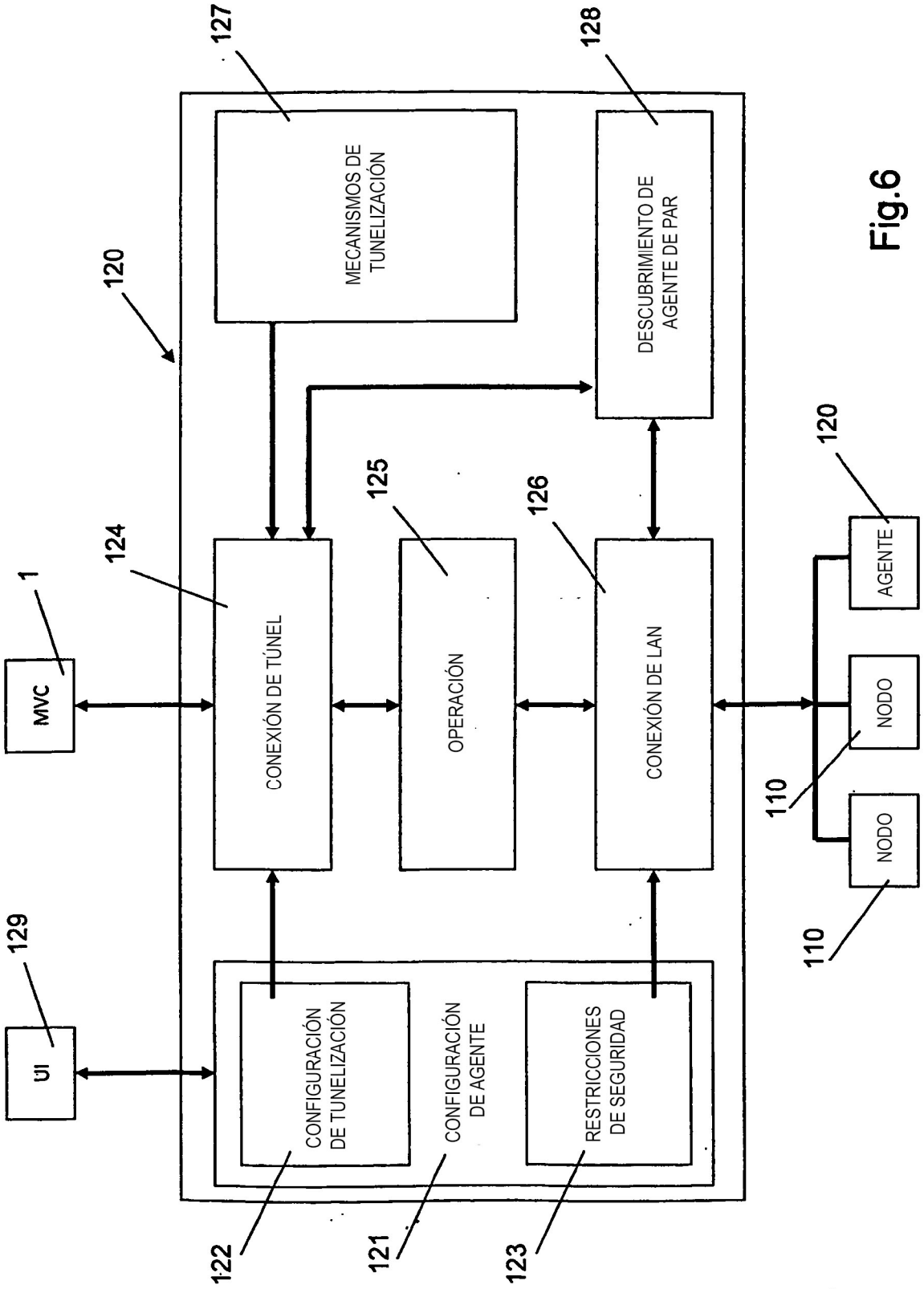
127
128
MECANISMOS DE TUNELIZACIÓN
DESCUBRIMIENTO DE AGENTE DE PAR
120
125
126
124
1
MVC
CONEXIÓN DE TÚNEL
OPERACIÓN
CONEXIÓN DE LAN
120
AGENTE
NODO
110
NODO
110
129
UI
CONFIGURACIÓN DE TUNELIZACIÓN
CONFIGURACIÓN DE AGENTE
RESTRICCIONES DE SEGURIDAD
122
121
123

Fig.6

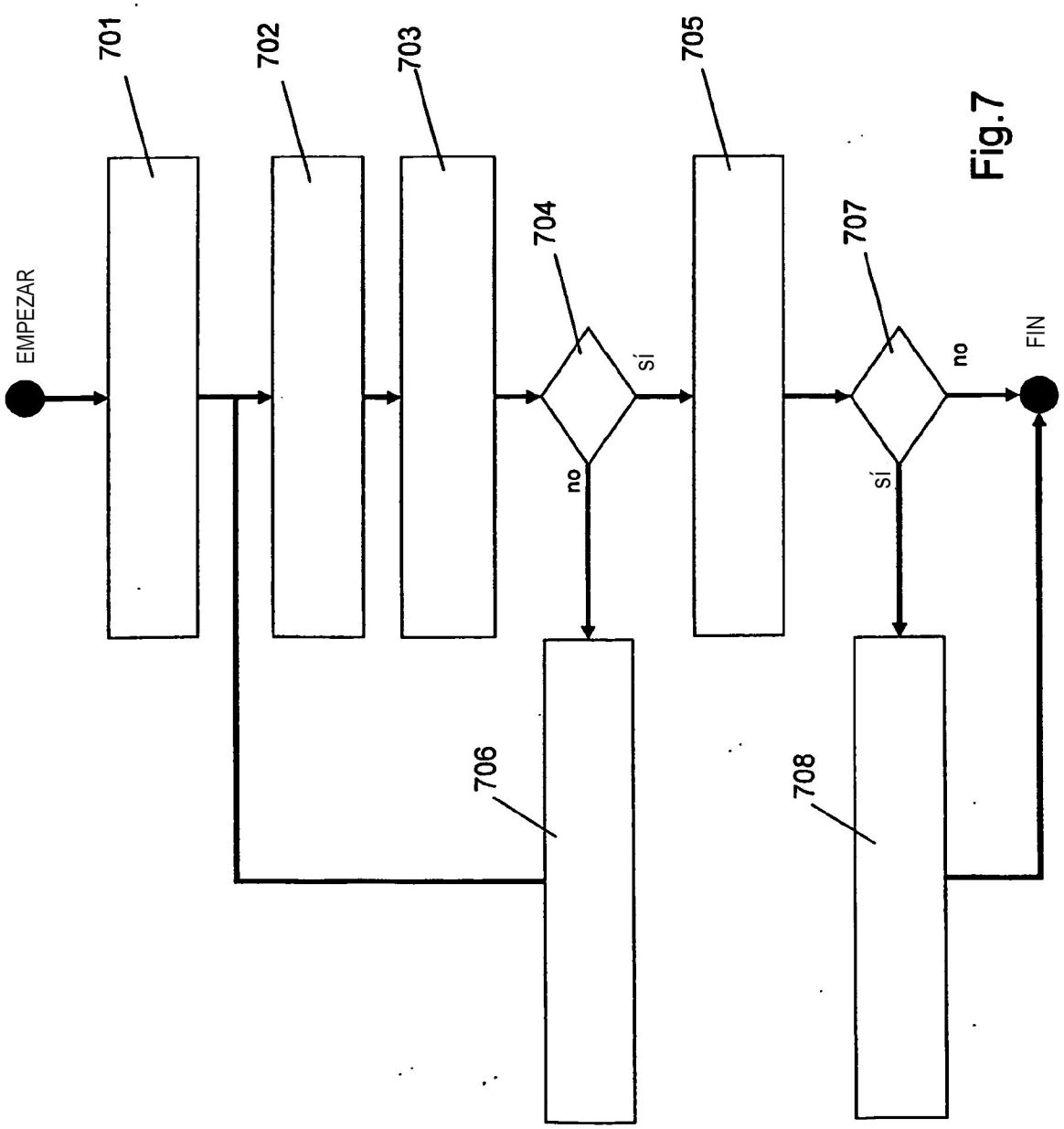


Fig.7

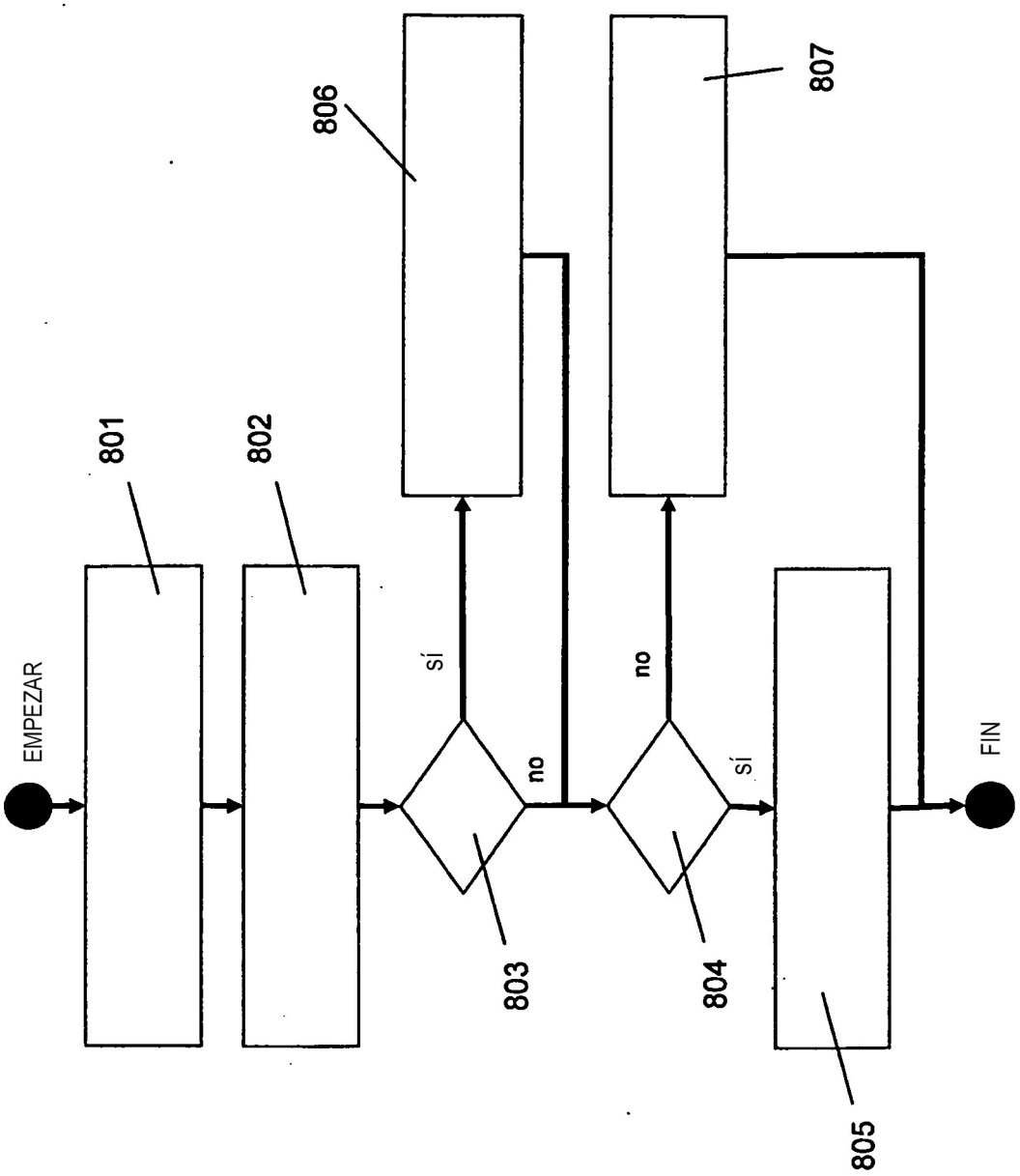


Fig.8

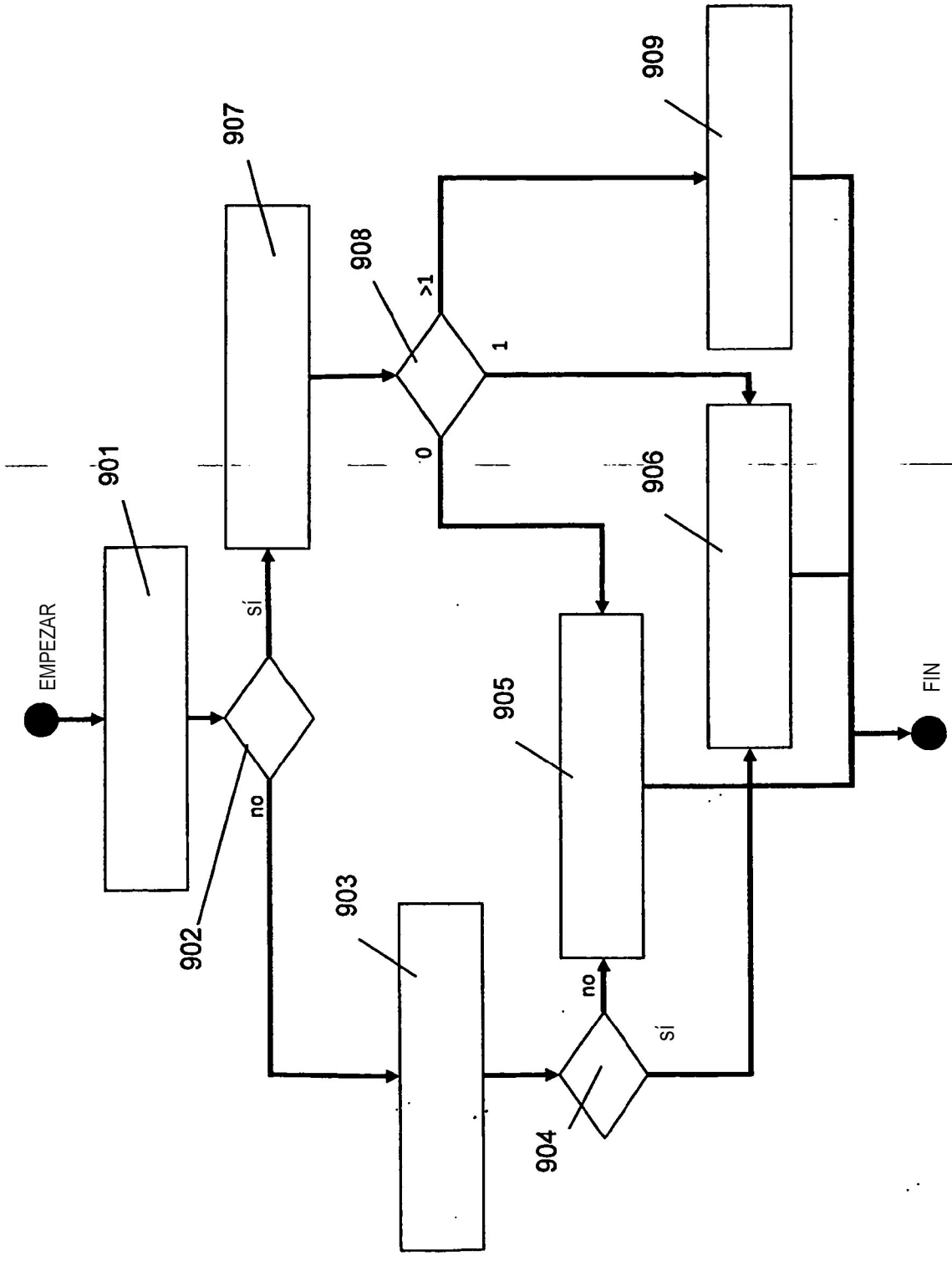


Fig.9

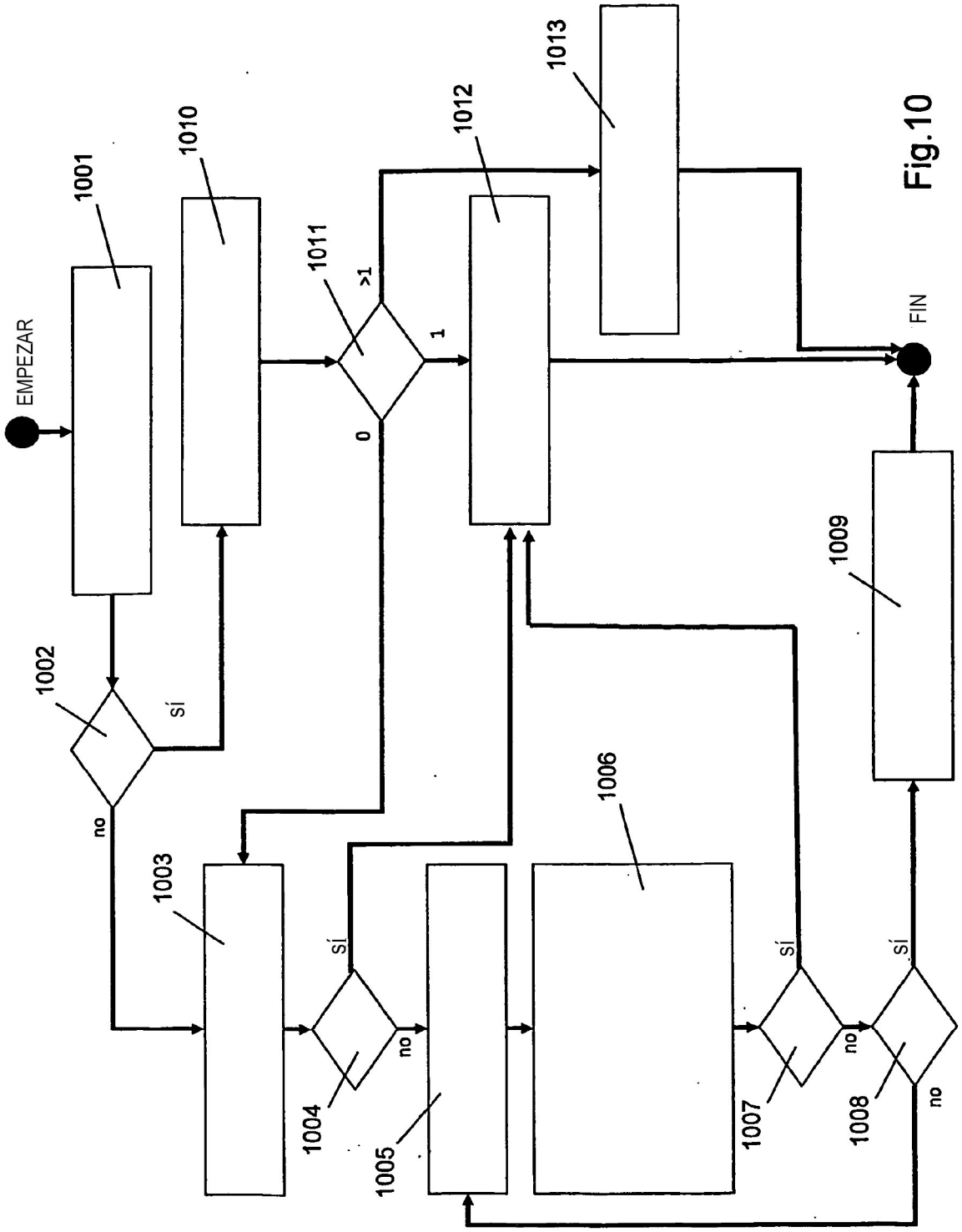
EMPEZAR
1001
1010
1011
>1
1
0
1012
1013
FIN
1009
1002
sí
no
1003
sí
1004
no
1005
1006
sí
1007
no
sí
1008
no

Fig.10

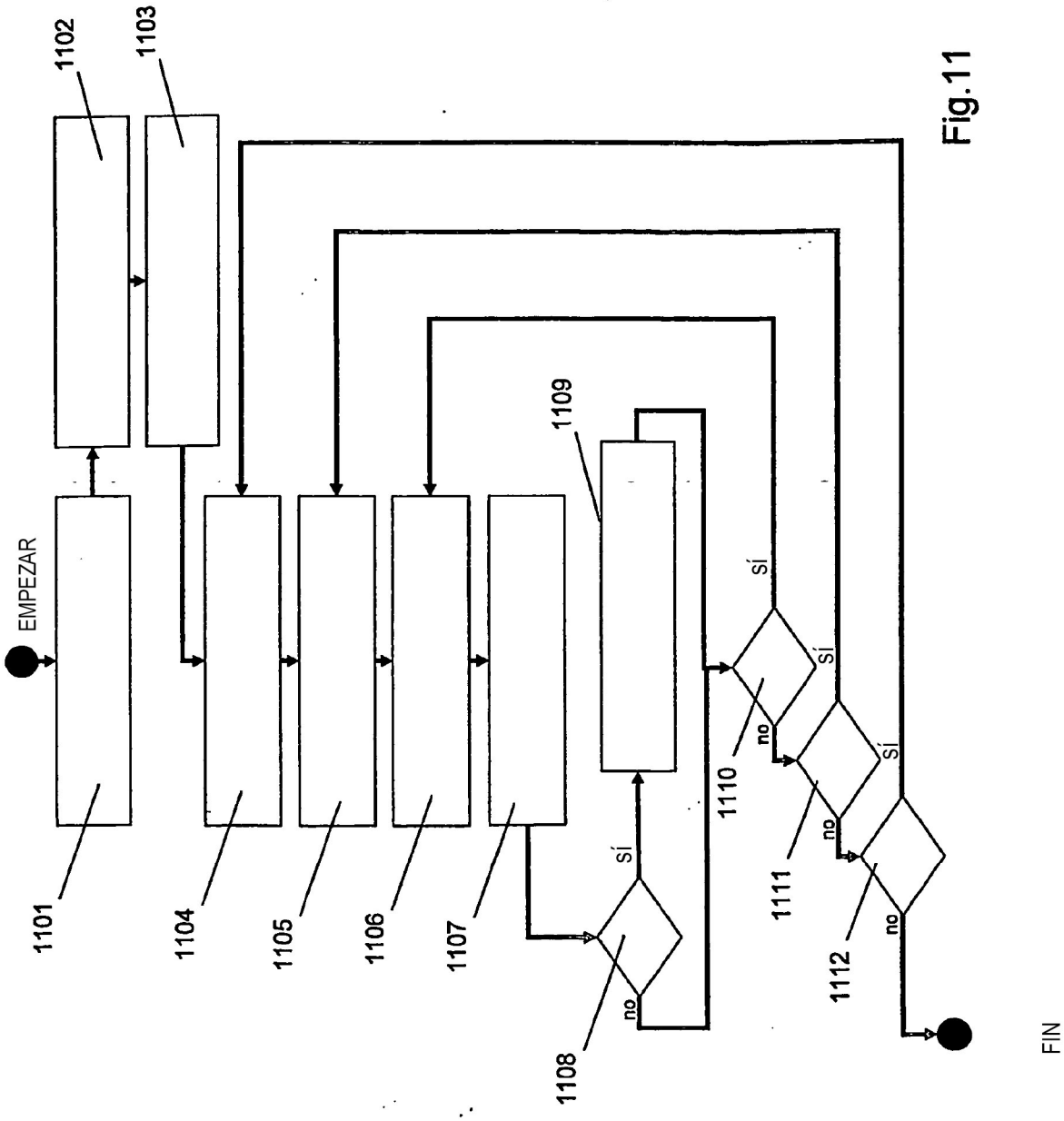
EMPEZAR
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
sí
no
FIN

Fig.11

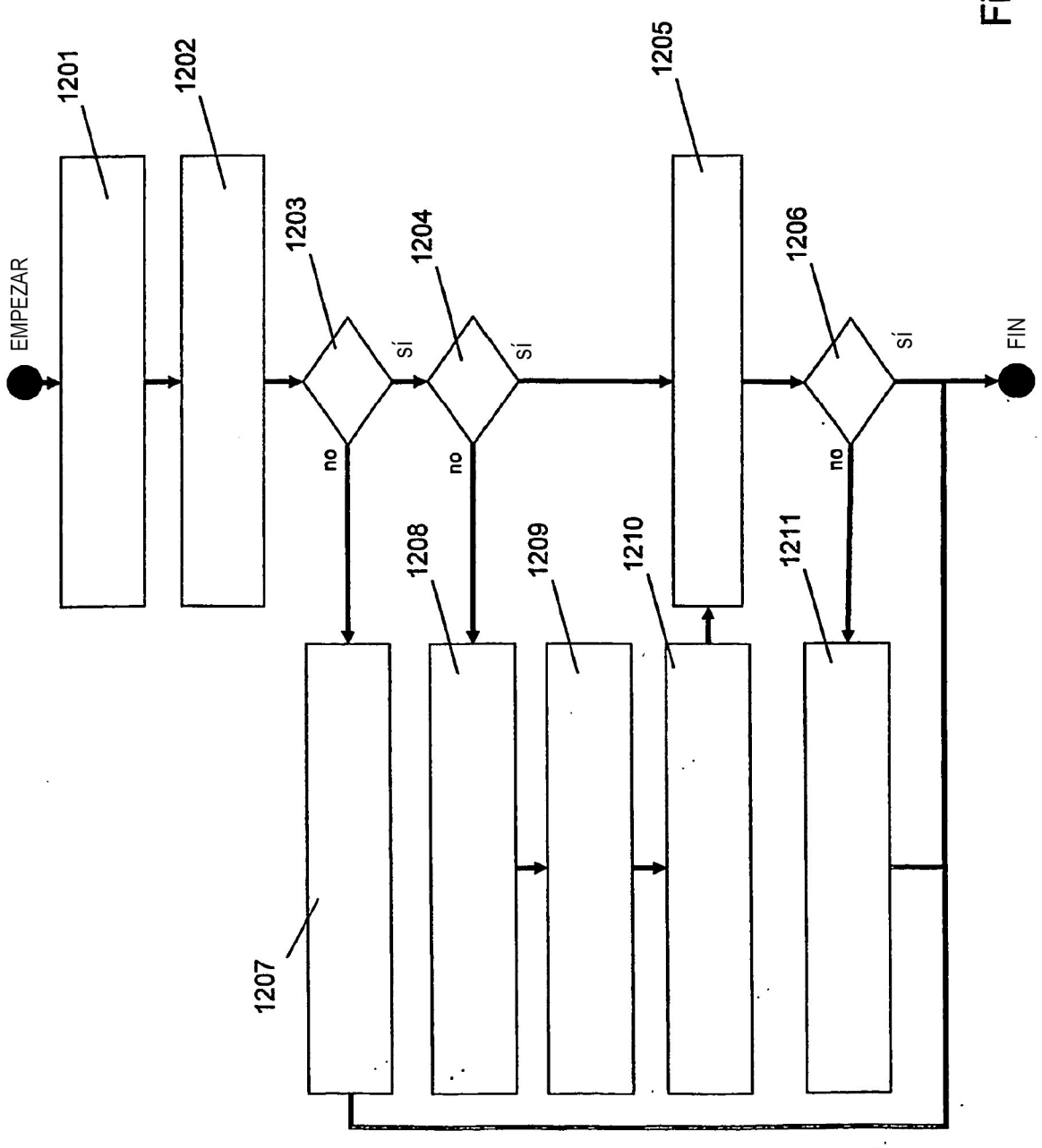
EMPEZAR
1201
1202
1203
sí
1204
sí
1205
1206
sí
FIN
no
no
no
1207
1208
1209
1210
1211

Fig.12

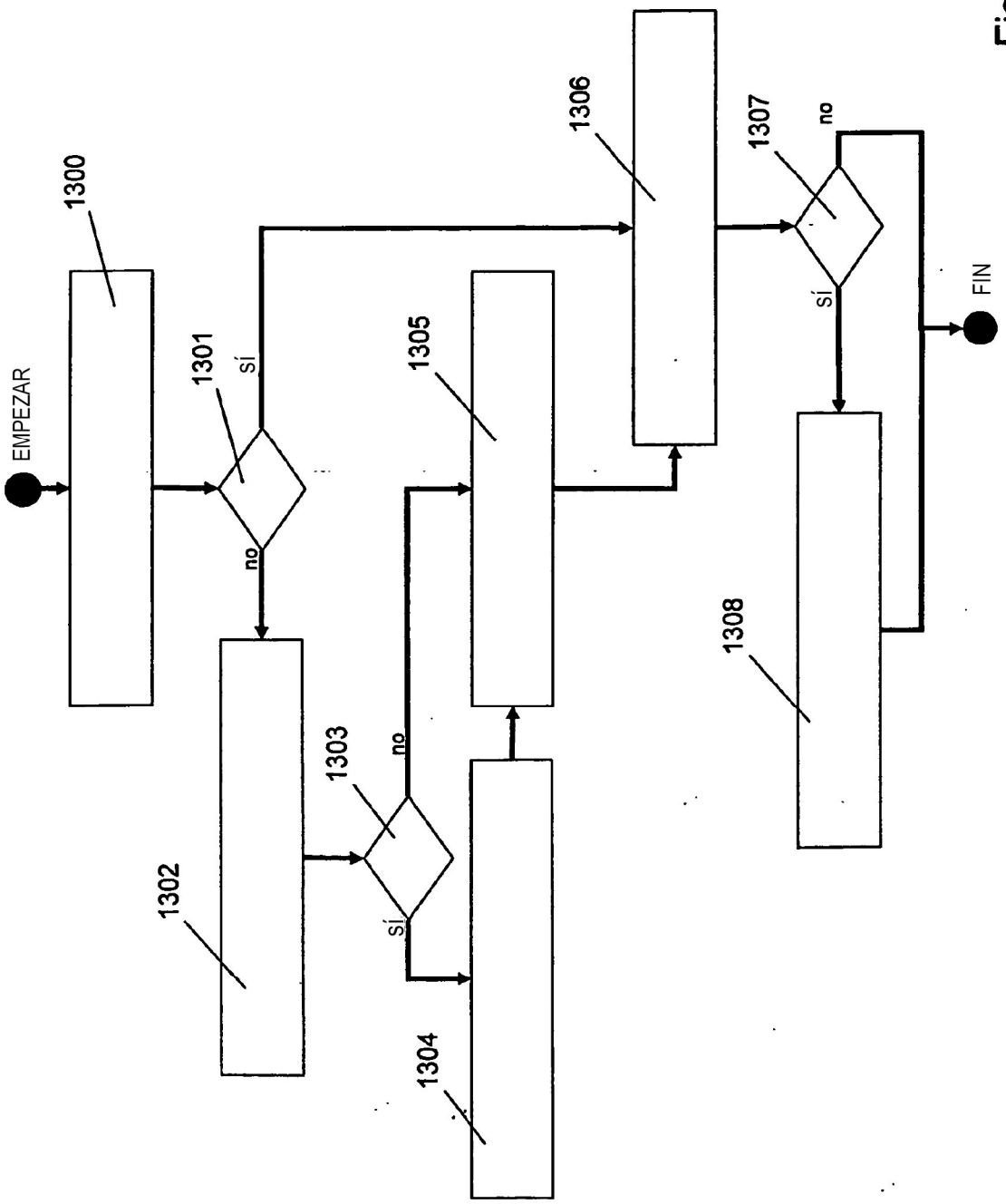
EMPEZAR
1300
1301
sí
no
1302
1303
no
sí
1304
1305
1306
1307
no
sí
1308
FIN

Fig.13

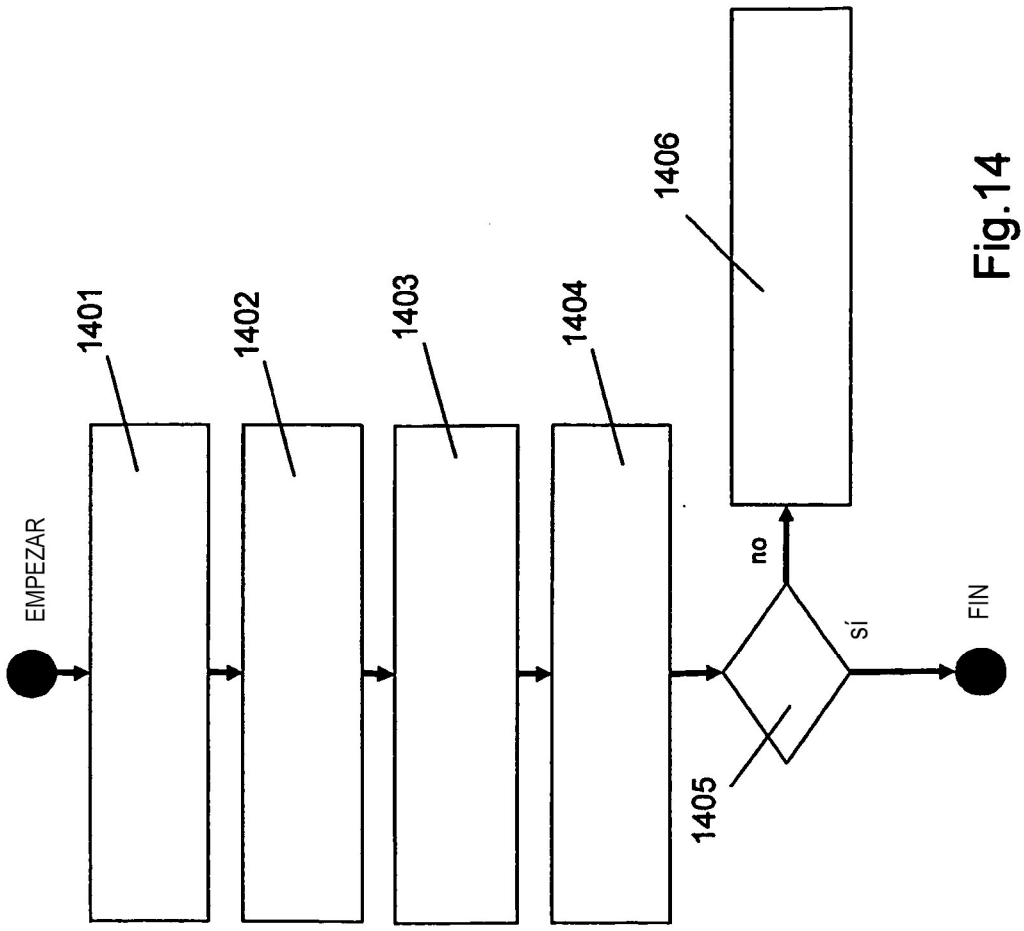


Fig.14

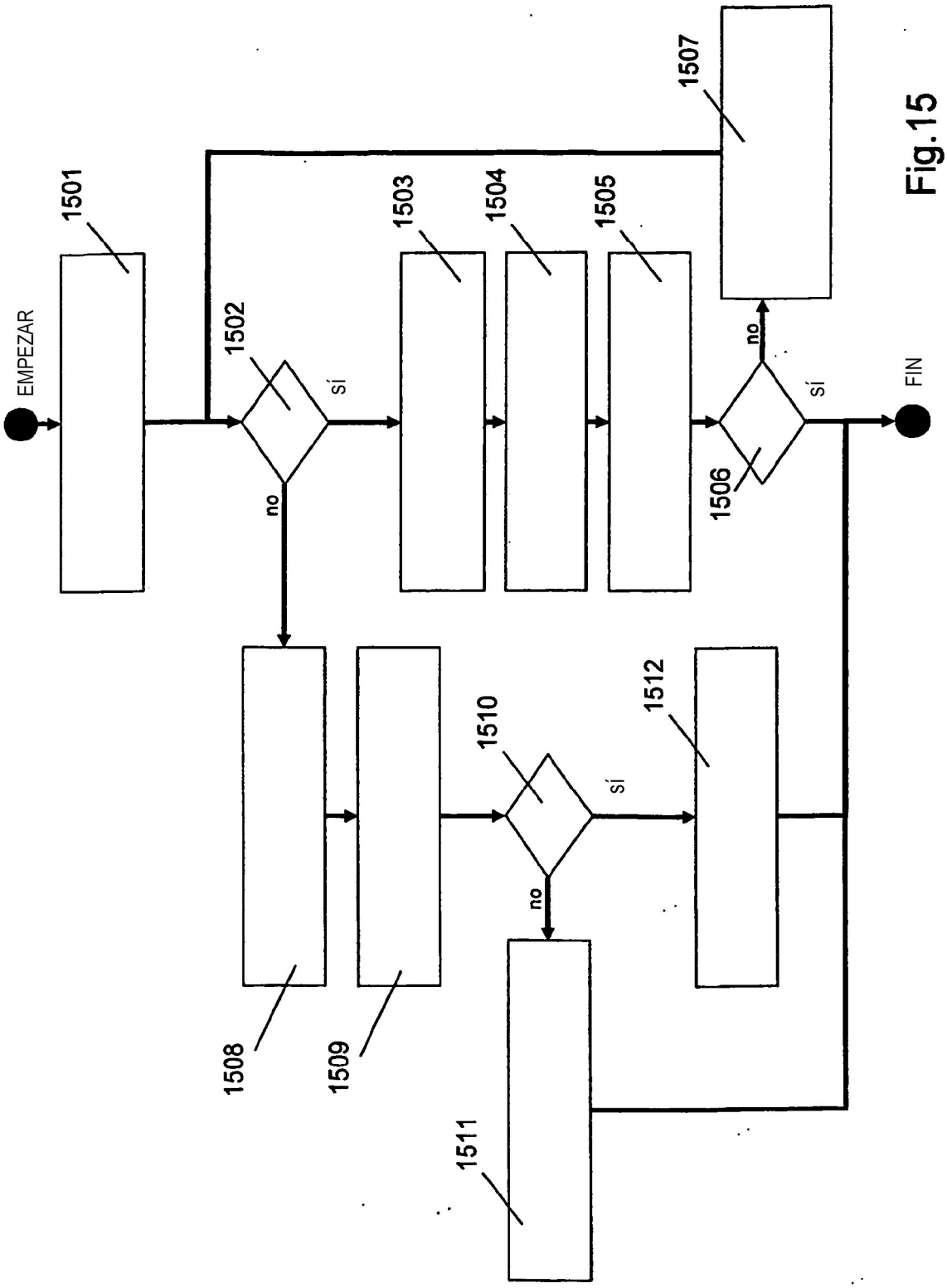
EMPEZAR
1501
1502
sí
no
1503
1504
1505
1506
no
sí
1507
FIN
1508
1509
1510
sí
no
1511
1512

Fig.15